TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Hilla Ryytty

Smithin normaalimuoto

Informaatiotieteiden yksikkö
Matematiikka
Huhtikuu 2015

Tampereen yliopisto
Informaatiotieteiden yksikkö
RYYTTY, HILLA: Smithin normaalimuoto
Pro gradu -tutkielma, 46 s.
Matematiikka
Huhtikuu 2015

Tiivistelmä

Tutkielmassa käsitellään aluksi euklidisia alueita, joista esimerkkejä ovat kuntakertoiminen polynomirengas ja Gaussin kokonaisluvut. Euklidisten alueiden merkittävä ominaisuus on se, että niiden jokainen ideaali on pääideaali. Näiden erityisten kokonaisalueiden jälkeen esitellään erilaisia matriisien samankaltaisuuteen viittaavia käsitteitä, joita ovat similaarisuus, R-ekvivalenttius, permutaatioekvivalenttius sekä Gaussin ekvivalenttius. Jälkimmäisen määrittelemiseksi tutustutaan kuitenkin ensin alkeisrivi- ja -sarakeoperaatioihin, jotka voi esittää sopivina matriisikertolaskuina. Smithin normaalimuodoksi kutsuttu tutkielman päätulos antaa euklidisten alueiden suhteen määritellyille nollamatriisista eroaville matriiseille mielenkiintoisen Gaussin ekvivalentin muodon. Lisäksi todistetaan, että R-ekvivalenttius ja Gaussin ekvivalenttius ovat yhtäpitävät ominaisuudet, mikäli R on euklidinen alue.

Alkeisoperaatioiden lisäksi matriisin invariantit tekijät eli käytännössä Smithin normaalimuoto on mahdollista selvittää tutkimalla minorien suurimpia yhteisiä tekijöitä. Tämän tuloksen seurauksena todetaan, että Smithin normaalimuoto on yksiköllä kertomista vaille yksikäsitteinen. Jos invariantit tekijät kuitenkin valitaan pääpolynomeiksi, Smithin normaalimuoto on täysin yksikäsitteinen. Kuntakertoimisista polynomeista koostuvat neliömatriisit $xI - A$ ja $xI - B$ todistetaan $F[x]$-ekvivalenteiksi, jos ja vain jos niiden Smithin normaalimuodot ovat samat. Alkeisjakajia käsitellään lyhyesti esimerkkien avulla. Viimeisessä luvussa tarkastellaan Smithin normaalimuodon alkuperäistä tarkoitusta lineaaristen Diofantoksen yhtälöryhmien ratkaisemisessa. Toisena sovelluksena tutkitaan kahden matriisin permutaatioekvivalenttiutta. Tutkielman pääteoksena käytetään Joseph J. Rotmanin teosta Advanced Modern Algebra.

Asiasanat: euklidinen alue, Gaussin ekvivalentti, Smithin normaalimuoto, invariantit tekijät

Sisältö

1 Johdanto

Henry John Stephen Smith (1826 – 1883) oli arvostettu brittiläismatemaatikko, joka toimi geometrian professorina Oxfordin yliopistossa. Tiettyjen geometristen näkökulmien lisäksi hänen erikoisalaansa oli etenkin lukuteoria, ja häntä pidettiinkin yhtenä aikansa parhaista lukuteoreetikoista. Vuonna 1861 Smith julkaisi ainoan artikkelinsa Smithin normaalimuodosta. Tämä artikkeli *On systems of linear indeterminate equations and congruences* syntyi hänen kiinnostuksestaan ratkaista lineaarisia Diofantoksen yhtälöryhmiä ja kongruensseja. Tästä alkoi Smithin normaalimuodon ja sen sovellusten tutkiminen (ks. [4, s. 557] ja [7, s. 367]).

Tutkielman ensimmäinen varsinainen luku esitietojen jälkeen käsittelee euklidisia alueita, jotka ovat astefunktiolla varustettuja jakoalgoritmin toteuttavia kokonaisalueita. Osoitetaan esimerkiksi, että kuntakertoiminen polynomirengas on euklidinen alue, kun astefunktio valitaan luonnollisesti. Toisena esimerkkinä esitetään Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$. Luvun lopuksi todistetaan, että jokainen euklidinen alue on pääideaalialue.

Seuraavaksi määritellään matriisien samankaltaisuutta kuvaavat käsitteet similaarisuus ja R-ekvivalenttius, jotka ovat ekvivalenssirelaatioita. Alkeisoperaatioiden esittelemisen jälkeen pystytään määrittelemään myös Gaussin ekvivalenttius, joka on keskeisessä osassa hieman myöhemmin käsiteltävän päätuloksen yhteydessä.

Luku 5 alkaa tutkielman keskeisimmällä lauseella, joka tunnetaan nimellä Smithin normaalimuoto. Sen mukaan kaikki nollamatriisista eroavat matriisit, joiden alkiot kuuluvat johonkin euklidiseen alueeseen, ovat Gaussin ekvivalentteja muotoa

$$\begin{pmatrix} \Sigma & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$$

olevan matriisin kanssa. Tässä $\mathbf{0}$ tarkoittaa nollalohkoa ja $\Sigma = \operatorname{diag}(\sigma_1, \sigma_2, \ldots, \sigma_q)$ lävistäjämatriisia, jossa nollasta poikkeaville lävistäjäalkioille $\sigma_1, \sigma_2, \ldots, \sigma_q$ pätee $\sigma_1 \mid \sigma_2 \mid \cdots \mid \sigma_q$. Luvun päätteeksi osoitetaan, että R-ekvivalenttius ja Gaussin ekvivalenttius ovat yhtäpitävät käsitteet, kun R on euklidinen alue.

Kuudes luku käsittelee invariantteja tekijöitä ja alkeisjakajia. Todistetaan lause, jonka mukaan invariantit tekijät (ja siis Smithin normaalimuoto) voidaan selvittää alkeisoperaatioiden sijaan tarkastelemalla minorien suurimpia yhteisiä tekijöitä. Tämän perusteella todetaan Smithin normaalimuodon olevan yksiköllä kertomista vaille yksikäsitteinen. Osoitetaan myös, että $F[x]$-ekvivalenteilla matriiseilla $xI - A$ ja $xI - B$ on sama Smithin normaalimuoto, kun A:n ja B:n alkiot kuuluvat kuntaan F.

Viimeisen luvun tarkoitus on näyttää konkreettisella tavalla, mihin Smithin normaalimuotoa voi esimerkiksi käyttää. Tarkastelussa ovat erityisesti lineaaristen Diofantoksen yhtälöryhmien ratkaiseminen sekä kahden matriisin permutaatioekvivalenttiuden selvittäminen.

Lukijan oletetaan tutustuneen kompleksilukuihin ja pienten matriisien determinanttien laskemiseen. Lisäksi hän ymmärtää, mitä suurimmalla yhteisellä tekijällä (syt) ja ilmaisulla ”a jakaa b:n” (merkitään $a \mid b$) tarkoitetaan. Myös polynomeja, matriisikertolaskua ja ekvivalenssirelaatiota käsitellään ilman tarkkaa esittelemistä.

2 Esitietoja

Tässä luvussa esitellään luettelonomaisesti myöhemmin tarvittavia algebrallisia ja lineaarialgebrallisia käsitteitä. Lisäksi osoitetaan muun muassa, että yksiköllisen vaihdannaisen renkaan kokonaisaluepiirre on yhtäpitävä supistussäännön voimassaolon kanssa ja että jokainen kunta on kokonaisalue.

2.1 Ryhmät ja renkaat

Aloitetaan määrittelemällä kaksi erittäin keskeistä algebrallista rakennetta – ryhmä ja rengas.

Määritelmä 2.1. Vrt. [8, s. 15]. Laskutoimituksella $*$ varustettu epätyhjä joukko G on *ryhmä*, jos se toteuttaa seuraavat ominaisuudet:

1) (*liitännäisyys*) kaikilla $a, b, c \in G$ pätee

$$(a * b) * c = a * (b * c),$$

2) (*neutraalialkio*) kaikille $a \in G$ on olemassa sellainen $e \in G$, että

$$e * a = a * e = a,$$

3) (*käänteisalkiot*) kaikille $a \in G$ on olemassa alkio $a^{-1} \in G$, jolle

$$a * a^{-1} = a^{-1} * a = e,$$

missä e on laskutoimituksen $*$ neutraalialkio.

Jos tarkastelemme laskutoimituksella $*$ varustettua ryhmää G, sitä voidaan merkitä $(G, *)$. Ryhmää $(G, *)$ kutsutaan *Abelin ryhmäksi*, mikäli kolmen edellä mainitun ominaisuuden lisäksi kaikille $a, b \in G$ pätee *vaihdantalaki* eli $a * b = b * a$.

Esimerkki 2.1. Yksinkertainen esimerkki ryhmästä on $(\mathbb{Z}, +)$. Olkoon $a \in \mathbb{Z}$. Kokonaislukujen yhteenlasku on tunnetusti liitännäinen, ja neutraalialkio on nolla, sillä $0 + a = a + 0 = a$. Käänteisalkiona (tai tässä vasta-alkiona) on puolestaan luvun a vastaluku $-a$, koska $a + (-a) = -a + a = 0$. Itse asiassa $(\mathbb{Z}, +)$ on lisäksi Abelin ryhmä, sillä kokonaislukujen yhteenlasku on myös vaihdannainen.

Sen sijaan havaitaan, että $(\mathbb{Z}, \cdot)$ ei ole ryhmä, koska vaikkapa luvulla $2 \in \mathbb{Z}$ ei ole käänteisalkiota kokonaislukujen joukossa. Kertolaskun neutraalialkio on ensinnäkin 1, sillä tiedetään, että $1 \cdot a = a \cdot 1 = a$. Luku $2m$ on parillinen kaikilla $m \in \mathbb{Z}$, mutta 1 on pariton, joten ei voi olla, että $2m = 1$.

Määritelmä 2.2. Vrt. [8, s. 16]. Kahdella laskutoimituksella varustettua epätyhjää rakennetta $(R, +, \cdot)$ kutsutaan *renkaaksi*, jos

1) $(R, +)$ on Abelin ryhmä,
2) (*liitännäisyys*) kaikilla $a, b, c \in R$ pätee

$$(ab)c = a(bc),$$

3) (*osittelulait*) kaikilla $a, b, c \in R$ pätevät ehdot

$$(a + b)c = ac + bc \quad \text{ja} \quad c(a + b) = ca + cb.$$

Jos kaikilla $a, b \in R$ pätee myös ominaisuus $ab = ba$, rengasta $(R, +, \cdot)$ kutsutaan *vaihdannaiseksi renkaaksi*. Rengas on *yksiköllinen*, mikäli se sisältää sellaisen alkion e, että $ae = ea = a$ kaikilla $a \in R$. Tähän yksikköön viitataan usein 1:llä. Rengasta $(R, +, \cdot)$ tavataan merkitä lyhyesti myös pelkällä R:llä.

Esimerkki 2.2. Vrt. [5, s. 263]. Olkoon R jatkuvien kuvausten joukko väliltä $[0, 1]$ reaalilukujen joukkoon. Jos kahden kuvauksen summa ja tulo määritellään luonnollisella tavalla $(f + g)(x) = f(x) + g(x)$ ja $(fg)(x) = f(x)g(x)$, R on yksiköllinen vaihdannainen rengas. Tarkistetaan tämä kohta kohdalta. Olkoot $f, g, h \in R$, ja olkoon $x \in [0, 1]$. Ensin on osoitettava, että $(R, +)$ on Abelin ryhmä. Liitännäisyys pätee, sillä

$$\begin{aligned}((f + g) + h)(x) &= (f + g)(x) + h(x) \\ &= \big(f(x) + g(x)\big) + h(x) \\ &= f(x) + \big(g(x) + h(x)\big) \\ &= f(x) + (g + h)(x) \\ &= \big(f + (g + h)\big)(x).\end{aligned}$$

Huomaa, että esimerkiksi $f(x)$ on reaaliluku, joten tarkasteluissa voidaan vedota reaalilukujen vastaaviin ominaisuuksiin. Neutraalialkiona on nollakuvaus. Tämä voidaan tarkistaa seuraavalla yhtälöketjulla:

$$(0+f)(x) = 0(x)+f(x) = 0+f(x) = f(x) = f(x)+0 = f(x)+0(x) = (f+0)(x).$$

Kuvauksen f käänteisalkio on $-f$, koska

$$\begin{aligned}\big(f + (-f)\big)(x) &= f(x) + (-f)(x) \\ &= f(x) - f(x) \\ &= 0(x) \\ &= -f(x) + f(x) \\ &= (-f + f)(x).\end{aligned}$$

Lisäksi yhteenlasku on vaihdannainen:

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x),$$

joten on saatu näytettyä, että $(R, +)$ on Abelin ryhmä.

Osoitetaan seuraavaksi kertolaskun liitännäisyys. Olkoot edelleen $f, g, h \in R$ jatkuvia kuvauksia, ja olkoon $x \in [0, 1]$. Tällöin

$$\begin{aligned}((fg)h)(x) &= (fg)(x)h(x)\\ &= \big(f(x)g(x)\big)h(x)\\ &= f(x)\big(g(x)h(x)\big)\\ &= f(x)(gh)(x)\\ &= \big(f(gh)\big)(x).\end{aligned}$$

Myös osittelulait pätevät, sillä

$$\begin{aligned}((f+g)h)(x) &= (f+g)(x)h(x)\\ &= \big(f(x)+g(x)\big)h(x)\\ &= f(x)h(x)+g(x)h(x)\\ &= (fh)(x)+(gh)(x)\\ &= (fh+gh)(x)\end{aligned}$$

ja

$$\begin{aligned}\big(h(f+g)\big)(x) &= h(x)(f+g)(x)\\ &= h(x)\big(f(x)+g(x)\big)\\ &= h(x)f(x)+h(x)g(x)\\ &= (hf)(x)+(hg)(x)\\ &= (hf+hg)(x).\end{aligned}$$

Nyt siis R on osoitettu renkaaksi. Tarkistetaan vielä, että se on yksiköllinen ja vaihdannainen. Yksikkönä on ykköskuvaus $1(x) = 1$:

$$(f \cdot 1)(x) = f(x) \cdot 1(x) = f(x) \cdot 1 = f(x) = 1 \cdot f(x) = 1(x) \cdot f(x) = (1 \cdot f)(x).$$

Kertolaskun vaihdannaisuus pätee reaalilukujen kertolaskun vaihdannaisuuden perusteella. Argumentti on siis sama kuin monessa muussakin kohdassa tässä esimerkissä. Yksinkertaisesti

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x).$$

Muistutuksena huomautettakoon, että *polynomirengas* $R[x]$ koostuu polynomeista, joiden kertoimet kuuluvat renkaaseen R. Polynomin määritelmä oletetaan lukijalle ennestään tutuksi.

Määritelmä 2.3. Vrt. [9, s. 91]. Olkoon $f(x) = a_0 + a_1x + \cdots + a_nx^n$ nollasta eroava polynomi. Tällöin on olemassa sellainen $n \geq 0$, että $a_n \neq 0$ ja $a_i = 0$ kaikilla $i > n$. Tällöin kerrointa a_n kutsutaan polynomin $f(x)$ *korkeimman asteen termin kertoimeksi* ja lukua n polynomin $f(x)$ *asteeksi*. Astetta merkitään $n = \deg\big(f(x)\big)$.

Huomautus. Määritellään, että nollapolynomilla 0 ei ole astetta, koska sillä ei ole yhtään nollasta poikkeavaa kerrointa. Monissa lähteissä määritellään kuitenkin, että $\deg(0) = -\infty$.

Huomautus. Jos polynomin korkeimman asteen termin kerroin on 1, polynomia sanotaan *pääpolynomiksi*.

Määritelmä 2.4. Vaihdannaisen renkaan R alkiota u sanotaan *yksiköksi*, mikäli on olemassa sellainen $v \in R$, että $uv = 1$.

Lause 2.5. (Jakoalgoritmi) *Olkoon R yksiköllinen vaihdannainen rengas. Olkoot $f(x), g(x) \in R[x]$ sellaisia polynomeja, että $f(x)$:n korkeimman asteen termin kerroin on yksikkö R:ssä. Tällöin on olemassa yksikäsitteiset polynomit $q(x) \in R[x]$ ja $r(x) \in R[x]$, joille pätee $g(x) = q(x)f(x) + r(x)$, missä joko $r(x) = 0$ tai* $\deg(r(x)) < \deg(f(x))$.

Todistus. Ks. esimerkiksi [6, s. 338–339]. □

2.2 Kokonaisalueet ja kunnat

Tarkastellaan rengasta R. Renkaan alkiota $r \in R$, $r \neq 0$, kutsutaan *nollanjakajaksi*, mikäli on olemassa nollasta poikkeava $s \in R$, jolle pätee $rs = 0$. Tästä päästään seuraavaksi kokonaisalueen käsitteeseen, joka on keskeinen muun muassa tulevassa euklidisen alueen määritelmässä.

Määritelmä 2.6. Vrt. [8, s. 17]. Olkoon R yksiköllinen vaihdannainen rengas. Jos R ei sisällä nollanjakajia, sitä kutsutaan *kokonaisalueeksi*.

Kokonaisluvut ovat tyyppiesimerkki kokonaisalueesta. Kokonaisalueen olisi voinut määritellä myös niin sanotun *supistussäännön* avulla:

$$\text{jos} \quad ab = ac \quad \text{ja} \quad a \neq 0, \quad \text{niin} \quad b = c,$$

missä a, b ja c ovat yksiköllisen vaihdannaisen renkaan R alkioita. Supistussääntö pätee siis kaikissa kokonaisalueissa. Esitetään tämä lauseena.

Lause 2.7. *Olkoon R yksiköllinen vaihdannainen rengas. Tällöin R on kokonaisalue, jos ja vain jos supistussääntö pätee R:ssä.*

Todistus. Vrt. [8, s. 17]. Oletetaan ensin, että R on kokonaisalue. Oletetaan myös, että $a, b, c \in R$ ja että ehdot $ab = ac$ ja $a \neq 0$ ovat voimassa. On osoitettava, että $b = c$. Kun otetaan huomioon, että tulon nollasääntö pätee kokonaisalueessa, saadaan seuraava päättelyketju: Oletuksen mukaan $ab = ac$ ja $a \neq 0$. Vähennetään yhtälöstä puolittain ac ja otetaan a yhteiseksi tekijäksi, jolloin $a(b - c) = 0$. Koska edelleen tiedetään, että $a \neq 0$, päätellään, että $b - c = 0$. Tästä seuraa, että $b = c$.

Oletetaan sitten, että supistussääntö on voimassa ja että $ab = 0$, kun $a, b \in R$. On osoitettava, että $a = 0$ tai $b = 0$. Voidaan tehdä oletus, että $a \neq 0$, jolloin päästään supistussäännön tuttuun muotoon sijoittamalla $c = 0$: $a \neq 0$ ja $ab = a0$. Oletusten nojalla $b = 0$. Täten R:ssä ei ole nollanjakajia, ja se on siis kokonaisalue. □

Seuraavat tulokset käsittelevät renkaan R ja polynomirenkaan $R[x]$ välistä suhdetta. Ensin osoitetaan, että renkaan R yksiköllisyydestä ja vaihdannaisuudesta seuraavat vastaavat ominaisuudet myös polynomirenkaalle $R[x]$. Sen jälkeen todistetaan, että mikäli rengas on kokonaisalue, myös polynomirengas on kokonaisalue.

Apulause 2.8. Jos R on yksiköllinen vaihdannainen rengas, niin $R[x]$ on yksiköllinen vaihdannainen rengas.

Todistus. Vrt. [6, s. 337]. Oletetaan, että R on yksiköllinen vaihdannainen rengas. Olkoot $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ja $g(x) = b_0 + b_1x + \cdots + b_mx^m$ kaksi polynomirenkaan $R[x]$ alkiota, joissa $a_i = 0$ ja $b_j = 0$, kun $i > n$ ja $j > m$. Olkoot lisäksi $f(x)g(x) = c_0 + c_1x + \cdots + c_tx^t$ ja $g(x)f(x) = d_0 + d_1x + \cdots + d_tx^t$. Cauchyn kertosäännön nojalla $c_j = \sum_{i=0}^{j} a_ib_{j-i}$ ja $d_j = \sum_{i=0}^{j} b_ia_{j-i}$. Koska kertolasku R:ssä on vaihdannainen, niin

$$\begin{aligned} c_j &= a_0b_j + a_1b_{j-1} + \cdots + a_jb_0 \\ &= a_jb_0 + a_{j-1}b_1 + \cdots + a_0b_j \\ &= b_0a_j + b_1a_{j-1} + \cdots + b_ja_0 \\ &= d_j \end{aligned}$$

kaikilla $j \in \mathbb{N}$. On osoitettu, että $f(x)g(x) = g(x)f(x)$, joten kertolasku $R[x]$:ssä on vaihdannainen. Koska $1 \in R$, niin myös $1 \in R[x]$, ja kaikilla $f(x) \in R[x]$ pätee $1 \cdot f(x) = f(x) \cdot 1 = f(x)$. Näin ollen $R[x]$ on yksiköllinen.

Täytyisi vielä varmistua, että polynomirengas $R[x]$ on rengas. Tarkat laskutoimitukset jätetään lukijalle. Yhteenlaskun liitännäisyys ja vaihdannaisuus voidaan todeta yhdistämällä polynomifunktioiden saman asteen termien kertoimet ja hyödyntämällä renkaan R vastaavia ominaisuuksia. Yhteenlaskun neutraalialkio on nollapolynomi. Polynomin $f(x)$ käänteisalkio puolestaan on $-f(x)$, missä jokaisen termin kerroin on polynomin $f(x)$ vastaavan termin kertoimen vastaluku. Myös kertolaskun liitännäisyyttä ja osittelulakeja tutkittaessa voi vedota siihen, että R on rengas, jossa siis kertolasku on liitännäinen ja osittelulait pätevät. Kokonaisuudessaan $R[x]$ on siis yksiköllinen vaihdannainen rengas. □

Lause 2.9. *Jos R on kokonaisalue, niin polynomirengas $R[x]$ on kokonaisalue.*

Todistus. Vrt. [6, s. 337]. Oletetaan, että R on kokonaisalue. Määritelmän 2.6 mukaan R on yksiköllinen vaihdannainen rengas. Apulauseen 2.8 perusteella puolestaan $R[x]$ on yksiköllinen vaihdannainen rengas. Olkoot $f(x) = a_0 + a_1x + \cdots + a_nx^n$ ja $g(x) = b_0 + b_1x + \cdots + b_mx^m$ kaksi nollasta eroavaa polynomirenkaan $R[x]$ alkiota. Tällöin on olemassa sellaiset kertoimet $a_i \neq 0$ ja $b_j \neq 0$, että $a_{i+t} = 0$ ja $b_{j+t} = 0$ kaikilla $t \geq 1$. Olkoon $f(x)g(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$. On osoitettava, että $f(x)g(x) \neq 0$ eli että polynomirenkaassa $R[x]$ ei ole nollanjakajia. Nyt polynomien kertolaskun perusteella

$$c_{i+j} = a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_ib_j + \cdots + a_{i+j}b_0 = a_ib_j \neq 0,$$

koska $a_i, b_j \in R \setminus \{0\}$ ja R on kokonaisalue. Täten vähintään yksi polynomin $f(x)g(x)$ kertoimista on erisuuri kuin nolla, minkä perusteella $f(x)g(x) \neq 0$. On saatu todistettua, että $R[x]$ on myös kokonaisalue. □

Määritelmä 2.10. Vrt. [8, s. 23]. Rakenne $(F, +, \cdot)$ on *kunta*, jos

1) $(F, +)$ on Abelin ryhmä,
2) $(F^*, \cdot)$ on Abelin ryhmä, missä $F^* = F \setminus \{0\}$,
3) (*osittelulait*) kaikille $a, b, c \in F$ pätevät osittelulait

$$(a + b)c = ac + bc \quad \text{ja} \quad c(a + b) = ca + cb.$$

Huomautus. Vaihtoehtoisesti voi määritellä, että kunta on yksiköllinen vaihdannainen rengas, jonka jokaisella nollasta poikkeavalla alkiolla on käänteisalkio.

Tavallisimpia esimerkkikuntia lienevät joukot $\mathbb{Q}, \mathbb{R}$ ja $\mathbb{C}$. Seuraava perustulos auttaa siirtymään tarkasteluissa kunnasta kokonaisalueeseen.

Lause 2.11. *Jokainen kunta on kokonaisalue.*

Todistus. Vrt. [9, s. 87]. Edellä olevan huomautuksen perusteella tiedetään, että jokainen kunta on yksiköllinen vaihdannainen rengas. Lauseen 2.7 nojalla riittää todeta, että supistussääntö pätee. Oletetaan, että kunnan alkioille a, b ja c pätee $ab = ac$ ja $a \neq 0$. Nyt

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = c,$$

koska jokaisella kunnan nollasta eroavalla alkiolla on käänteisalkio kunnassa. □

On kuitenkin huomattava, että käänteinen tulos ei pidä paikkaansa. Esimerkiksi $\mathbb{Z}$ on kokonaisalue, mutta ei kunta. Katso myös esimerkki 2.1.

Määritelmä 2.12. Ks. [9, s. 327]. Kunta F on *algebrallisesti suljettu*, mikäli jokaisella $F[x]$:n polynomilla, joka ei ole vakio, on juuri kunnassa F.

Perusesimerkkinä algebrallisesti suljetusta kunnasta voi pitää kompleksilukujen kuntaa. Reaalilukujen kunta ei puolestaan ole algebrallisesti suljettu, sillä muun muassa polynomilla $x^2 + 1$ ei ole reaalisia juuria.

2.3 Ideaalit ja pääideaalialueet

Seuraavaksi määritellään ideaalin ja pääideaalialueen käsitteet. Myöhemmin alaluvussa 3.3 huomataan, että jokainen euklidinen alue on nimenomaan pääideaalialue.

Määritelmä 2.13. Vrt. [8, s. 18]. Vaihdannaisen renkaan R epätyhjää osajoukkoa $I \subseteq R$ kutsutaan *ideaaliksi*, mikäli seuraavat ehdot pätevät:

1) jos $a \in I$ ja $b \in I$, niin $a - b \in I$,
2) jos $a \in I$ ja $r \in R$, niin $ra \in I$.

Yhden alkion virittämä ideaali on nimeltään *pääideaali*. Se voidaan esittää muodossa $\langle a \rangle = \{ra \mid r \in R\}$, kun $a \in R$ ja R on yksiköllinen vaihdannainen rengas. Mikäli yksiköllisen vaihdannaisen renkaan jokainen ideaali on pääideaali, se on *pääideaalirengas*. Kirjoitetaan vastaava määritelmä myös kokonaisalueille.

Määritelmä 2.14. Vrt. [8, s. 19]. Jos kokonaisalue on pääideaalirengas, sitä kutsutaan *pääideaalialueeksi*.

Esimerkki 2.3. Kokonaislukujen rengas $(\mathbb{Z}, +, \cdot)$ on pääideaalialue, sillä kuten aikaisemmin todettiin, se on kokonaisalue, ja lisäksi sen jokainen ideaali on pääideaali. Tämä johtuu siitä, että kokonaislukujen renkaan kaikki *aliryhmät* ovat muotoa $n\mathbb{Z} = \langle n \rangle$, missä n on jokin kokonaisluku. Renkaan ideaaleiksi kelpaavat nimittäin ainoastaan sen aliryhmät.

2.4 Matriisit

Tässä alaluvussa esitellään kertauksenomaisesti matriiseihin liittyviä peruskäsitteitä. Lukijan odotetaan kuitenkin hallitsevan matriisikertolaskun ennestään. Alaluvussa noudatetaan pitkälti Serge Langin määritelmiä (ks. [5, s. 37–40, 48]).

Määritelmä 2.15. Tarkastellaan yksiköllistä vaihdannaista rengasta R ja kahta kokonaislukua $m, n \geq 1$. Renkaan R alkioiden muodostamaa rakennetta

$$A = [a_{ij}] = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

kutsutaan *matriisiksi*. Tällä matriisilla on m *riviä* ja n *saraketta*, ja sitä voikin nimittää $m \times n$*-matriisiksi*. Merkitään $A \in M_{mn}(R)$.

Esimerkki 2.4. *Nollamatriisi* O on matriisi, jolla on alkionaan ainoastaan nollia. Esimerkiksi 2×4-kokoinen nollamatriisi on muotoa

$$O = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Määritelmä 2.16. Jos matriisin rivien ja sarakkeiden lukumäärät ovat samat, niin matriisi on *neliömatriisi*. Merkitään R-alkioisten $n \times n$-matriisien joukkoa $M_n(R)$.

Neliömatriisit ovat kiinnostavia jo siksi, että niille voidaan laskea *determinantit*. Determinantin määrittäminen ainakin 2×2- ja 3×3-matriiseille oletetaan tässä yhteydessä tunnetuksi. Matriisin A determinanttia merkitään $\det(A)$. Kun A on neliömatriisi, polynomia $\det(xI - A)$ kutsutaan matriisin A *karakteristiseksi polynomiksi* ja merkitään $\mathrm{ch}(A)$. A:n *minimaalipolynomilla* $\min(A)$ tarkoitetaan puolestaan pieniasteisinta pääpolynomia $f(x)$, jolle pätee $f(A) = 0$.

Määritelmä 2.17. Vrt. [9, s. 734]. Olkoon $A \in M_{mn}(R)$, missä R on yksiköllinen vaihdannainen rengas. Tarkastellaan seuraavaa kahta joukkoa: $H = \{i_1, i_2, \dots, i_p\}$ ja $L = \{j_1, j_2, \dots, j_p\}$, missä on oltava $1 \leq p \leq \min\{m, n\}$. Oletetaan alkioiden olevan erisuuria ja nousevassa järjestyksessä. Toisin sanoen $1 \leq i_1 < i_2 < \cdots < i_p \leq m$ ja $1 \leq j_1 < j_2 < \cdots < j_p \leq n$. Nyt $A_{H,L}$ on matriisin A $p \times p$-kokoinen *alimatriisi* $[a_{st}]$, missä $(s, t) \in H \times L$. Tällaisen $p \times p$-alimatriisin determinanttia kutsutaan *p:nnen kertaluvun minoriksi*.

Huomautus. Alimatriisi $A_{H,L}$ saadaan matriisista A poistamalla kaikki i:nnet rivit, missä $i \notin H$, ja j:nnet sarakkeet, missä $j \notin L$.

Luvussa 6 käytetään määritelmän 2.17 käsitteiden lisäksi matriisin A *transpoosia* $A^\top$. Transpoosi saadaan matriisista A vaihtamalla sen rivit sarakkeiksi.

Määritelmä 2.18. Neliömatriisia sanotaan *lävistäjämatriisiksi*, mikäli se on muotoa

$$\begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & d_n \end{pmatrix}.$$

Ylläolevaa matriisia voidaan merkitä *lävistäjällä* eli *diagonaalilla* olevien alkioiden $d_1, d_2, \dots, d_n$ mukaan $\operatorname{diag}(d_1, d_2, \dots, d_n)$ (engl. *diagonal matrix*). Huomaa, että lävistäjän ulkopuolella on pelkkiä nollia. Myös lävistäjällä voi toki esiintyä nolla-alkioita.

Identiteettimatriisi I_n tai lyhyesti I on erikoistapaus $n \times n$-lävistäjämatriisista. Siinä lävistäjäalkiot ovat ykkösiä, ja muualla on lävistäjämatriisin määritelmän mukaan pelkkiä nollia.

Joskus on tarpeen laskea $n \times n$-neliömatriisin A *jälki* (engl. *trace*) $\operatorname{tr}(A)$, joka saadaan lävistäjäalkioiden a_{ii} summana:

$$\operatorname{tr}(A) = \sum_{i=1}^{n} a_{ii}.$$

Huomaa, että jälkeä laskettaessa kyseessä ei kuitenkaan tarvitse olla lävistäjämatriisi. Identiteettimatriisin tapauksessa $\operatorname{tr}(I_n) = n$. Siirrytään seuraavaksi niin sanottuihin kääntyviin matriiseihin, joita käsiteltäessä matriisikertolasku on tunnettava.

Määritelmä 2.19. Vrt. [9, s. 738]. Olkoon R yksiköllinen vaihdannainen rengas ja A $n \times n$-matriisi, jonka alkiot kuuluvat R:ään. Tällöin A on *kääntyvä*, jos on olemassa sellainen matriisi B, että

$$AB = I = BA.$$

Tässä myös B:n alkiot kuuluvat renkaaseen R, ja B:tä kutsutaan A:n *käänteismatriisiksi*.

Huomautus. Jos matriisilla A on käänteismatriisi, se on yksikäsitteinen ja sitä merkitään A^{-1}.

Huomautus. Kääntyvillä matriiseilla on aina nollasta poikkeava determinantti.

Lause 2.20. *Olkoon R yksiköllinen vaihdannainen rengas ja $A \in M_n(R)$. Tällöin jos A on kääntyvä, niin* $\det(A)$ *on yksikkö R:ssä.*

Todistus. Vrt. [9, s. 739]. Oletetaan, että A on kääntyvä. Määritelmän mukaan on siis olemassa matriisi B, joka toteuttaa yhtälön $AB = I$. Käyttämällä kahta tuttua determinantin ominaisuutta, $\det(I) = 1$ ja $\det(AB) = \det(A)\det(B)$, päätellään

$$1 = \det(I) = \det(AB) = \det(A)\det(B).$$

Määritelmän 2.4 nojalla $\det(A)$ on yksikkö R:ssä. □

Huomautus. Lauseen 2.20 tulos pätee myös käänteisesti. Esimerkiksi neliömatriisi $A \in M_n(\mathbb{Z})$ on kääntyvä, jos ja vain jos $\det(A) = \pm 1$ (ks. [4, s. 558]).

Määritelmä 2.21. Vrt. [2, s. 87]. Olkoon A $m \times n$-matriisi. Matriisin A *asteella* tarkoitetaan suurinta sellaista kokonaislukua p, että on olemassa nollasta poikkeava p:nnen kertaluvun minori. Matriisi itse kelpaa myös tarkasteltavaksi alimatriisiksi, mikäli se on neliömatriisi. Matriisin A astetta merkitään $\operatorname{rank}(A)$.

Esimerkki 2.5. Määritetään seuraavan matriisin aste:

$$A = \begin{pmatrix} 5 & 1 & 2 & 0 \\ 8 & 0 & 4 & 6 \\ 4 & 3 & 7 & 1 \end{pmatrix}.$$

Havaitaan ensin, että $1 \leq \operatorname{rank}(A) \leq 3$. Ainoastaan nollamatriisilla on asteenaan nolla. Toisaalta aste ei voi olla neljä, koska A:ssa on vain kolme riviä. Lähdetään kokeilemaan suurinta vaihtoehtoa. Koska

$$\det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & 6 \\ 3 & 7 & 1 \end{pmatrix} = 1 \cdot \det \begin{pmatrix} 4 & 6 \\ 7 & 1 \end{pmatrix} - 2 \cdot \det \begin{pmatrix} 0 & 6 \\ 3 & 1 \end{pmatrix} = 4 - 42 - 2 \cdot (-18) = -2 \neq 0,$$

asteeksi saadaan $\operatorname{rank}(A) = 3$. Tässä esimerkissä on mahdollista valita 3×3-alimatriisi neljällä eri tavalla. Mikäli jokainen niistä olisi tuottanut determinantiksi nollan, olisi täytynyt ruveta tarkastelemaan pienempiä 2×2-alimatriiseja, jolloin asteeksi olisi ollut mahdollista saada enintään kaksi.

3 Euklidiset alueet

3.1 Euklidisen alueen määritelmä

Epämuodollisesti voisi määritellä, että euklidinen alue on jakoalgoritmin toteuttava kokonaisalue. Esimerkiksi polynomeja voi tunnetusti jakaa jakokulmassa. Merkittävää jakoalgoritmissa on, että tällöin jaettavan polynomin aste putoaa koko ajan, kunnes algoritmi väistämättä pysähtyy. Jakokulma-ajattelua jatkaen loppujen lopuksi jakojäännökseksi saadaan jokin polynomi, jonka aste on pienempi kuin jakajan aste.

Määritelmä 3.1. Vrt. [6, s. 345] ja [9, s. 124]. *Euklidinen alue* $(E, +, \cdot, \partial)$ on kokonaisalue $(E, +, \cdot)$, joka on varustettu sellaisella funktiolla $\partial : E \setminus \{0\} \to \mathbb{N}$, että seuraavat ehdot pätevät:

(i) $\partial(f) \leq \partial(fg)$ kaikilla $f, g \in E \setminus \{0\}$,

(ii) Jakoalgoritmi on voimassa: kaikilla $f, g \in E$, $f \neq 0$, on olemassa alkiot $q, r \in E$, jotka toteuttavat yhtälön $g = qf + r$, missä joko $r = 0$ tai $\partial(r) < \partial(f)$.

Huomautus. Määritelmässä 3.1 esiintyvää funktiota ∂ kutsutaan *astefunktioksi*. Jos se on *multiplikatiivinen* eli $\partial(fg) = \partial(f)\partial(g)$ kaikilla $f, g \in E \setminus \{0\}$, niin ∂ on *normi*. Usein puhutaan lyhyesti vain euklidisesta alueesta E.

Seuraavaksi tarkastellaan paria perusesimerkkiä euklidisista alueista. Aikaisemmin monessa kohtaa käytetty yksinkertainen esimerkkirengas $\mathbb{Z}$ on myös esimerkki euklidisesta alueesta, kunhan astefunktio ∂ valitaan sopivasti. Tietyissä tapauksissa myös polynomirengas täyttää euklidisen alueen kriteerit. Tämä esitetään lauseen muodossa.

Esimerkki 3.1. (1) Rengas $\mathbb{Z}$ ja funktio $\partial : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, missä $\partial(a) = |a|$, muodostavat euklidisen alueen. Alaluvun 2.2 lopuksi todettiin ensinnäkin, että $\mathbb{Z}$ on kokonaisalue. Kaikilla $a, b \in \mathbb{Z} \setminus \{0\}$

$$\partial(a) = |a| \leq |a||b| = |ab| = \partial(ab),$$

sillä $|b| \geq 1$, ja täten euklidisen alueen määritelmän ensimmäinen ehto täyttyy. Myös toinen ehto toteutuu, sillä tunnetusti renkaassa $\mathbb{Z}$ toimii jakoalgoritmi.

(2) $\mathbb{Z}$:lle voisi valita astefunktioksi myös vaikkapa funktion $\partial : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$, missä $\partial(a) = a^2$. Samalla perusteella kuin kohdassa (1) saadaan euklidisen alueen määritelmän toinen kriteeri täytettyä. Myös ensimmäinen ehto on voimassa: Olkoot $a, b \in \mathbb{Z} \setminus \{0\}$. Tällöin

$$\partial(a) = a^2 \leq a^2 b^2 = (ab)^2 = \partial(ab),$$

koska tässä $b^2 \geq 1$.

Esimerkki 3.2. Vrt. [6, s. 346]. Kunta F on euklidinen alue, kun se varustetaan funktiolla $\partial : F \setminus \{0\} \to \mathbb{N}, \partial(a) = 1$. Lauseen 2.11 nojalla F on myös kokonaisalue. Määritelmän 3.1 ehto (i) on tietenkin voimassa, sillä $\partial(a) = 1 \leq 1 = \partial(ab)$, kun $a, b \in F \setminus \{0\}$. Tarkastellaan sitten alkioita $c, d \in F$, missä $c \neq 0$. Koska F on kunta, jokaisella sen nollasta poikkeavalla alkiolla on käänteisalkio kunnassa. Siis on olemassa $c^{-1} \in F$, jolle pätee $cc^{-1} = c^{-1}c = 1$. Nyt alkio d voidaan esittää muodossa

$$d = (dc^{-1})c + 0,$$

minkä perusteella voi sanoa, että jakoalgoritmi toteutuu. Täten F on euklidinen alue.

Lause 3.2. *Jos F on kunta, niin polynomirengas $F[x]$ on euklidinen alue.*

Todistus. Vrt. [6, s. 345–346]. Oletetaan, että F on kunta. Lauseen 2.11 nojalla F on myös kokonaisalue ja edelleen lauseen 2.9 perusteella $F[x]$ on kokonaisalue. Määritellään astefunktio kuten nollasta eroavan polynomin aste yleensä (ks. myös määritelmä 2.3):

$$\partial : F[x] \setminus \{0\} \to \mathbb{N}, \quad \partial(f(x)) = \deg(f(x)).$$

Tässä koska $\deg(f(x)) \geq 0$, niin $\partial(f(x)) \in \mathbb{N}$ kaikilla $f(x) \in F[x] \setminus \{0\}$.

Aloitetaan määritelmän 3.1 kohdalla (i). Olkoot $f(x) = a_0 + a_1x + \cdots + a_nx^n$, missä $a_n \neq 0$, ja $g(x) = b_0 + b_1x + \cdots + b_mx^m$, missä $b_m \neq 0$, polynomirenkaan $F[x] \setminus \{0\}$ polynomeja. Tällöin $f(x)g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_mx^{n+m}$. F on kuntana myös kokonaisalue, joten $a_nb_m \neq 0$, koska kokonaisalueessa ei ole nollanjakajia. Siksi $\deg(f(x)g(x)) = n + m$. Nyt

$$\partial(f(x)) = \deg(f(x)) = n \leq n + m = \deg(f(x)g(x)) = \partial(f(x)g(x)).$$

Todistetaan seuraavaksi kohta (ii). Olkoot $f(x) \neq 0$ ja $g(x)$ polynomirenkaan $F[x]$ polynomeja. Koska jokainen nollasta poikkeava kunnan alkio on yksikkö, polynomin $f(x)$ korkeimman asteen termin kerroin on yksikkö F:ssä. Voidaan käyttää lausetta 2.5, jonka nojalla on olemassa sellaiset polynomit $q(x), r(x) \in F[x]$, että

$$g(x) = q(x)f(x) + r(x),$$

missä joko $r(x) = 0$ tai $\deg(r(x)) < \deg(f(x))$. Astefunktion määritelmästä seuraa, että

$$g(x) = q(x)f(x) + r(x),$$

missä joko $r(x) = 0$ tai $\partial(r(x)) < \partial(f(x))$. Täten $F[x]$ on euklidinen alue. □

Lauseen 3.2 perusteella esimerkiksi reaalilukukertoiminen polynomirengas $\mathbb{R}[x]$ on euklidinen alue, kun valitaan astefunktioksi polynomin asteen palauttava kuvaus.

3.2 Gaussin kokonaisluvut euklidisena alueena

Aloitetaan tämä alaluku määrittelemällä Gaussin kokonaisluvut. Oletuksena on, että lukijalla on perustiedot kompleksiluvuista. Käsite määritellään, koska se tuo mukanaan lisäesimerkkejä euklidisista alueista.

Määritelmä 3.3. Kompleksilukujen osajoukkoa $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ kutsutaan *Gaussin kokonaislukujen* joukoksi.

Huomautus. Äskeisessä määritelmässä i:n paikalla esiintyy usein jokin muu luku. Esimerkiksi $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

Esimerkki 3.3. Osoitetaan seuraavaa lausetta ajatellen, että Gaussin kokonaislukujen joukko $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ on kokonaisalue. Tämän voisi osoittaa hyvin lyhyesti: koska $\mathbb{C}$ on kokonaisalue ja tunnetusti $\mathbb{Z}[i] \subseteq \mathbb{C}$ on rengas, täytyy myös $\mathbb{Z}[i]$:n olla kokonaisalue. Osoitetaan joukko $\mathbb{Z}[i]$ kokonaisalueeksi kuitenkin määritelmän nojalla. Gaussin kokonaislukujen joukon ykkösalkio on $1 = 1 + 0i$ ja kertolasku on vaihdannainen, sillä tiedetään, että kompleksilukujen kertolasku on vaihdannainen ja $\mathbb{Z}[i] \subseteq \mathbb{C}$. Täten $\mathbb{Z}[i]$ on yksiköllinen vaihdannainen rengas.

Olkoot $a + bi, c + di \in \mathbb{Z}[i] \setminus \{0\}$, missä $0 = 0 + 0i$. Tällöin siis $a \neq 0$ tai $b \neq 0$ ja lisäksi $c \neq 0$ tai $d \neq 0$. Nyt on osoitettava, että tulo $(a + bi)(c + di) \neq 0$. Tehdään vastaoletus, että $(a + bi)(c + di) = 0$. Kompleksilukujen kertolaskun määritelmän nojalla saadaan, että

$$ac - bd + (ad + bc)i = 0,$$

joten päästään ratkaisemaan yhtälöparista

$$\begin{cases} ac - bd = 0 \\ ad + bc = 0 \end{cases}$$

kokonaislukujen $a, b, c, d \in \mathbb{Z}$ arvoja. Kertomalla ensin ylemmän yhtälön luvulla $-d$ ja alemman luvulla c päädytään tilanteeseen $b(c^2 + d^2) = 0$. Kokonaislukujen rengas on kokonaisalue, joten tulon nollasääntö on voimassa. Siksi $b = 0$ tai $c^2 + d^2 = 0$. Jälkimmäisestä seuraa kuitenkin, että $c = d = 0$, mikä ei voi pitää paikkaansa. Täten on oltava, että $b = 0$. Kerrotaan seuraavaksi alkuperäisen yhtälöparin ensimmäinen yhtälö luvulla c ja toinen yhtälö luvulla d. Tällä kertaa tuloksena on $a(c^2 + d^2) = 0$. Vastaavasti kuin äsken päätellään, että $a = 0$ tai $c^2 + d^2 = 0$. Jälleen jälkimmäinen vaihtoehto täytyy sulkea pois. Siis $a = 0$. Tämä on ristiriita, sillä oletettiin, että $a \neq 0$ tai $b \neq 0$. Siis $(a + bi)(c + di) \neq 0$, ja $\mathbb{Z}[i]$ on kokonaisalue. □

Seuraavaksi näytetään, että Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$ on euklidinen alue, kun sille valitaan sopiva astefunktio.

Lause 3.4. *Gaussin kokonaislukujen rengas $\mathbb{Z}[i]$ on euklidinen alue, kun astefunktiona on*

$$\partial : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}, \quad \partial(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

Todistus. Vrt. [9, s. 126]. Esimerkin 3.3 perusteella $\mathbb{Z}[i]$ on kokonaisalue. Huomattakoon, että astefunktio on normi: Olkoot $a + bi, c + di \in \mathbb{Z}[i] \setminus \{0\}$. Tällöin

$$\begin{aligned}\partial((a+bi)(c+di)) &= \partial(ac-bd+(ad+bc)i)\\ &= (ac-bd)^2+(ad+bc)^2\\ &= (ac)^2-2abcd+(bd)^2+(ad)^2+2abcd+(bc)^2\\ &= (ac)^2+(ad)^2+(bc)^2+(bd)^2\\ &= a^2c^2+a^2d^2+b^2c^2+b^2d^2\\ &= (a^2+b^2)(c^2+d^2)\\ &= \partial(a+bi)\partial(c+di).\end{aligned}$$

Tämän perusteella saadaan $\partial(a+bi) \leq \partial((a+bi)(c+di))$, koska $\partial(c+di) \geq 1$.

Osoitetaan vielä, että ∂ toteuttaa jakoalgoritmin. Tarkastellaan Gaussin kokonaislukuja $a+bi, c+di \in \mathbb{Z}[i]$, missä $a+bi \neq 0$. Merkitään tästä eteenpäin $\delta = c+di$ ja $\beta = a+bi$ ja otetaan käyttöön kompleksiluvun β liittoluku $\bar{\beta} = a-bi$. Nyt

$$\frac{\delta}{\beta} = \frac{\delta\bar{\beta}}{\beta\bar{\beta}} = \frac{\delta\bar{\beta}}{\partial(\beta)},$$

joten osamäärä $\delta/\beta = x+yi$, missä $x, y \in \mathbb{Q}$. Kirjoitetaan $x = s+u$ ja $y = t+v$, missä $s \in \mathbb{Z}$ on rationaalilukua x lähimpänä oleva kokonaisluku ja vastaavasti $t \in \mathbb{Z}$ on lukua y lähimpänä oleva kokonaisluku. Näin ollen $|u|, |v| \leq \frac{1}{2}$. Mikäli x tai y on muotoa $m+\frac{1}{2}$, missä m on kokonaisluku, lähimmäksi kokonaisluvuksi voi valita joko luvun m tai $m+1$. Uusien merkintöjen seurauksena saadaan

$$\frac{\delta}{\beta} = (s+u)+(t+v)i \quad \Leftrightarrow \quad \delta = \beta(s+u)+\beta(t+v)i = (s+ti)\beta+\beta(u+vi).$$

Selvästi $\delta = (s+ti)\beta+\beta(u+vi)$ on jakoyhtälömuodossa, kun vieläpä havaitsee, että $\beta(u+vi) \in \mathbb{Z}[i]$. Tämä pätee siksi, että $\beta(u+vi) = \delta-(s+ti)\beta$ ja kahden joukkoon $\mathbb{Z}[i]$ kuuluvan alkion tulo sekä erotus kuuluvat edelleen joukkoon $\mathbb{Z}[i]$.

Osoitetaan lopuksi, että $\partial(\beta(u+vi)) < \partial(\beta)$. Koska ∂ on multiplikatiivinen eli normi, niin

$$\partial(\beta(u+vi)) = \partial(\beta)\partial(u+vi).$$

Kuten aikaisemmin todettiin, $|u|, |v| \leq \frac{1}{2}$, joten $u^2, v^2 \leq \frac{1}{4}$. Tästä voidaan päätellä, että $\partial(u+vi) = u^2+v^2 \leq \frac{1}{4}+\frac{1}{4} = \frac{1}{2} < 1$. Edelleen $\partial(\beta(u+vi)) < \partial(\beta)$. On osoitettu, että $\mathbb{Z}[i]$ on euklidinen alue. □

Esimerkki 3.4. Vrt. [6, s. 350–351]. Osoitetaan, että $\mathbb{Z}[\sqrt{2}]$ on euklidinen alue, kun astefunktioksi asetetaan $\partial : \mathbb{Z}[\sqrt{2}]\setminus\{0\} \to \mathbb{N}$, $\partial(a+b\sqrt{2}) = \left|a^2-2b^2\right|$. Samaan tapaan kuin esimerkissä 3.3 voidaan osoittaa, että $\mathbb{Z}[\sqrt{2}]$ on kokonaisalue. Tässä voidaan vedota useiden laskulakien tarkistuksessa reaalilukujen vastaaviin ominaisuuksiin, sillä $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$.

Todistetaan määritelmän 3.1 kohta (i). Olkoot $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$. Nyt $\left|c^2-2d^2\right| \geq 1$. Ensinnäkin itseisarvo on aina luonnollinen luku. Lisäksi koska $c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$, joko $c \neq 0$ tai $d \neq 0$. Oletetaan, että $d \neq 0$ (tapaus $c \neq 0$ vastaavasti). Jos kuitenkin pätisi $\left|c^2-2d^2\right| = 0$, niin

$$\begin{aligned} c^2 - 2d^2 = 0 \quad &\Leftrightarrow \\ c^2 = 2d^2 \quad &\Leftrightarrow \\ \frac{c^2}{d^2} = 2 \quad &\Leftrightarrow \\ \left(\frac{c}{d}\right)^2 = 2 \quad &\Leftrightarrow \\ \frac{c}{d} = \sqrt{2}. \end{aligned}$$

Tämä ei kuitenkaan ole mahdollista, sillä $c, d \in \mathbb{Z}$, joten $\frac{c}{d} \in \mathbb{Q}$. Sen sijaan tunnetusti $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. Koska siis $\left|c^2 - 2d^2\right| \geq 1$, saadaan

$$\begin{aligned} \partial(a + b\sqrt{2}) &= \left|a^2 - 2b^2\right| \\ &\leq \left|a^2 - 2b^2\right|\left|c^2 - 2d^2\right| \\ &= \left|(a^2 - 2b^2)(c^2 - 2d^2)\right| \\ &= \left|(ac)^2 - 2(ad)^2 - 2(bc)^2 + 4(bd)^2\right| \\ &= \left|(ac + 2bd)^2 - 2(ad + bc)^2\right| \\ &= \partial((ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= \partial((a + b\sqrt{2})(c + d\sqrt{2})). \end{aligned}$$

Siirrytään seuraavaksi todistamaan määritelmän kohtaa (ii). Tarkastellaan alkioita $a + b\sqrt{2}$, $c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, missä $a + b\sqrt{2} \neq 0$. Pyritään osoittamaan, että on olemassa sellaiset alkiot $q_0 + q_1\sqrt{2}, r_0 + r_1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, että

$$c + d\sqrt{2} = (q_0 + q_1\sqrt{2})(a + b\sqrt{2}) + (r_0 + r_1\sqrt{2}),$$

missä joko $r_0 + r_1\sqrt{2} = 0$ tai $\left|r_0^2 - 2r_1^2\right| < \left|a^2 - 2b^2\right|$. Jos renkaassa $\mathbb{Z}[\sqrt{2}]$ on olemassa tällainen $q_0 + q_1\sqrt{2}$, niin silloin $\mathbb{Q}[\sqrt{2}]$:ssa pätee

$$\begin{aligned} r_0 + r_1\sqrt{2} &= (c + d\sqrt{2}) - (q_0 + q_1\sqrt{2})(a + b\sqrt{2}) \\ &= (a + b\sqrt{2})\Big((c + d\sqrt{2})(a + b\sqrt{2})^{-1} - (q_0 + q_1\sqrt{2})\Big). \end{aligned}$$

Merkitään $(c + d\sqrt{2})(a + b\sqrt{2})^{-1} = u + v\sqrt{2}$, missä $u, v \in \mathbb{Q}$. Jatketaan edelleen päättelyketjua:

$$\begin{aligned} r_0 + r_1\sqrt{2} &= (a + b\sqrt{2})\Big((u + v\sqrt{2}) - (q_0 + q_1\sqrt{2})\Big) \\ &= (a + b\sqrt{2})\Big((u - q_0) + (v - q_1)\sqrt{2}\Big) \\ &= \Big(a(u - q_0) + 2b(v - q_1)\Big) + \Big(a(v - q_1) + b(u - q_0)\Big)\sqrt{2}. \end{aligned}$$

Hyödynnetään seuraavassa tietoa, että esitys $a + b\sqrt{2}$ on yksikäsitteinen $\mathbb{Q}[\sqrt{2}]$:ssa. Huomataan, että jos $\left|(u - q_0)^2 - 2(v - q_1)^2\right| < 1$, niin

$$
\begin{aligned}
\left|r_0^2 - 2r_1^2\right| &= \left|\Big(a(u-q_0) + 2b(v-q_1)\Big)^2 - 2\Big(a(v-q_1) + b(u-q_0)\Big)^2\right| \\
&= \left|a^2(u-q_0)^2 + 4ab(u-q_0)(v-q_1) + 4b^2(v-q_1)^2\right. \\
&\quad \left. - 2a^2(v-q_1)^2 - 4ab(u-q_0)(v-q_1) - 2b^2(u-q_0)^2\right| \\
&= \left|a^2(u-q_0)^2 + 4b^2(v-q_1)^2 - 2a^2(v-q_1)^2 - 2b^2(u-q_0)^2\right| \\
&= \left|(a^2 - 2b^2)\Big((u-q_0)^2 - 2(v-q_1)^2\Big)\right| \\
&= \left|a^2 - 2b^2\right|\left|(u-q_0)^2 - 2(v-q_1)^2\right| \\
&< \left|a^2 - 2b^2\right|.
\end{aligned}
$$

On siis etsittävä sellainen alkio $q_0 + q_1\sqrt{2}$, että $\left|(u-q_0)^2 - 2(v-q_1)^2\right| < 1$. Olkoot $q_0, q_1 \in \mathbb{Z}$ sellaisia kokonaislukuja, että $(u-q_0)^2 \leq \frac{1}{4}$ ja $(v-q_1)^2 \leq \frac{1}{4}$. Tällöin voidaan päätellä, että

$$
-\frac{1}{2} \leq (u-q_0)^2 - 2(v-q_1)^2 \leq \frac{1}{4}.
$$

Tämän perusteella haluttu ehto $\left|(u-q_0)^2 - 2(v-q_1)^2\right| < 1$ pätee. On siis osoitettu, että on olemassa sellaiset $q_0 + q_1\sqrt{2}, r_0 + r_1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, että

$$
c + d\sqrt{2} = (q_0 + q_1\sqrt{2})(a + b\sqrt{2}) + (r_0 + r_1\sqrt{2}),
$$

missä $r_0 + r_1\sqrt{2} = 0$ tai $\left|r_0^2 - 2r_1^2\right| < \left|a^2 - 2b^2\right|$. Täten $\mathbb{Z}[\sqrt{2}]$ on euklidinen alue. □

3.3 Euklidisen alueen ideaalit

Tässä alaluvussa käsitellään lyhyesti euklidisten alueiden ideaaleja. Keskeisimpänä tuloksena esitetään, että jokainen euklidisen alueen ideaaleista on pääideaali. Perusteiden kertaamiseksi katso tarvittaessa alaluku 2.3.

Lause 3.5. *Jokainen euklidinen alue on pääideaalialue.*

Todistus. Vrt. [6, s. 348] ja [9, s. 125]. Olkoon E euklidinen alue, jonka astefunktio on ∂. Olkoon I euklidisen alueen E mielivaltainen ideaali. Koska E on yksiköllinen vaihdannainen rengas, riittää osoittaa, että I on pääideaali eli että $I = \langle a \rangle$ jollain $a \in E$. Jos $I = \{0\}$, niin I on nollan virittämä pääideaali eli $I = \langle 0 \rangle$, joten väite pätee.

Oletetaan sitten, että $I \neq \{0\}$. Tällöin ideaalissa I on vähintään yksi nollasta poikkeava alkio. Merkitään $P = \{\partial(x) \mid 0 \neq x \in I\}$. Havaitaan, että P on epätyhjä ja $P \subseteq \mathbb{N}$. Hyvinjärjestysperiaatteen mukaan joukossa P on oltava pienin alkio: on siis olemassa $0 \neq d \in I$, jolle pätee, että $\partial(d) \geq 0$ ja kaikilla nollasta poikkeavilla $a \in I$ $\partial(d) \leq \partial(a)$.

Olkoon $b \in \langle d \rangle$. Koska E on kokonaisalue ja täten yksiköllinen vaihdannainen rengas, saadaan, että $b = cd$, missä $c \in E$ ja $d \in I$. Määritelmän 2.13 kohdan 2) nojalla $cd = b \in I$. Näin ollen $\langle d \rangle \subseteq I$.

Oletetaan seuraavaksi, että $b \in I \subseteq E$. Koska E on euklidinen alue, on olemassa sellaiset alkiot $q, r \in E$, että $b = qd + r$ ja joko $r = 0$ tai $\partial(r) < \partial(d)$. Mutta nyt

$r = b - qd \in I$, koska ideaalin määritelmän nojalla ensinnäkin $qd \in I$, mistä seuraa, että myös $b - qd \in I$. Jos $r \neq 0$, niin $\partial(r) \in P$. Tämä on kuitenkin ristiriitaista, sillä nyt pätisi $\partial(r) < \partial(d)$ ja oletettiin, että alkiolla d on pienin aste joukossa P. On siis oltava, että $r = 0$, joten $b = qd \in \langle d \rangle$. Täten $I \subseteq \langle d \rangle$.

Kokonaisuudessaan ollaan päädytty tulokseen $I = \langle d \rangle$. Koska I on euklidisen alueen E mielivaltainen ideaali, jokainen E:n ideaaleista on pääideaali. Koska lisäksi E on kokonaisalue, se on pääideaalialue. □

Lauseen 3.5 mukaan siis esimerkiksi $\mathbb{Z}$, kuntakertoiminen polynomirengas $F[x]$ ja $\mathbb{Z}[i]$ ovat pääideaalialueita. Seuraava lause kokoaa kolme keskenään ekvivalenttia ominaisuutta.

Lause 3.6. *Olkoon R yksiköllinen vaihdannainen rengas. Tällöin seuraavat ehdot ovat yhtäpitävät:*

1) R on kunta.
2) $R[x]$ on euklidinen alue.
3) $R[x]$ on pääideaalialue.

Todistus. Vrt. [6, s. 348]. Käytetään hyväksi kahta aikaisemmin todistettua lausetta. Ensin havaitaan, että lauseen 3.2 perusteella kohdasta 1 seuraa kohta 2. Äsken todistetun lauseen 3.5 nojalla puolestaan kohdasta 2 seuraa kohta 3. Riittää siis osoittaa, että kohdasta 3 seuraa kohta 1.

Oletetaan, että $R[x]$ on pääideaalialue. On osoitettava, että tällöin R on kunta. Käytetään tässä määritelmän 2.10 jälkeen huomautuksessa esitettyä vaihtoehtoista kunnan määritelmää. Oletuksen nojalla R on yksiköllinen vaihdannainen rengas. Osoitetaan, että jokainen nollasta poikkeava renkaan R alkio on yksikkö eli sillä on käänteisalkio R:ssä.

Olkoon $a \in R$ ja $a \neq 0$. Olkoon $I = \langle a, x \rangle$ puolestaan alkioiden a ja x virittämä polynomirenkaan $R[x]$ ideaali. Koska $R[x]$ on pääideaalialue, on olemassa jokin sellainen $f(x) \in R[x]$, että $I = \langle f(x) \rangle$. Nyt tietenkin $a, x \in \langle f(x) \rangle$. Näin ollen täytyy olla olemassa sellaiset polynomit $g(x), h(x) \in R[x]$, että $f(x)g(x) = a$ ja $f(x)h(x) = x$. Koska $f(x)g(x) = a$, niin $\deg\big(f(x)g(x)\big) = 0$. Määritelmän 2.3 nojalla aste on ei-negatiivinen luku. Toisaalta voidaan olettaa tunnetuksi, että $\deg\big(f(x)g(x)\big) = \deg\big(f(x)\big) + \deg\big(g(x)\big)$, joten erityisesti $\deg\big(f(x)\big) = 0$. Täten $f(x) \in R$ ja voidaan kirjoittaa muodossa $f(x) = b \in R$.

Ehdosta $bh(x) = x$ voidaan päätellä, että $bc = 1$, missä $c \in R$ on polynomin $h(x)$ termin x kerroin. Täten b on yksikkö, ja $I = \langle b \rangle = R[x]$. Koska $R[x]$ on kokonaisalue, se on yksiköllinen, ja siksi $1 \in R[x] = I$. Siis alkio 1 voidaan esittää muodossa

$$1 = af_1(x) + xf_2(x)$$

joillakin $f_1(x), f_2(x) \in R[x]$. Nyt $1 = ad$, missä $d \in R$ on polynomin $f_1(x)$ vakiotermi. On saatu, että a on yksikkö R:ssä, mistä seuraa, että R on kunta. □

Esimerkki 3.5. Kokonaislukujen joukko $\mathbb{Z}$ on yksiköllinen vaihdannainen rengas, mutta se ei ole kunta. Siksi edellä esitetyn lauseen 3.6 perusteella voidaan päätellä, ettei polynomirengas $\mathbb{Z}[x]$ ole pääideaalialue.

4 Matriisien ekvivalenttius

Tässä luvussa tutustutaan enimmäkseen kahteen erilaiseen matriisien ekvivalenttiuteen: niin sanottuun R-ekvivalenttiuteen ja Gaussin ekvivalenttiuteen. Myöhemmin luvussa 5 käy kuitenkin ilmi, että nämä käsitteet ovat yhtäpitäviä euklidisissa alueissa. Lisäksi esitellään käsitteet similaarisuus ja permutaatioekvivalenttius.

4.1 R-ekvivalenttius

Ennen tämän alaluvun pääkäsitteen määrittelemistä esitellään kolmas matriisien ”samanlaisuuteen” viittaava käsite. Ekvivalenssirelaation määritelmä oletetaan seuraavassa tunnetuksi.

Määritelmä 4.1. Vrt. [9, s. 153]. Olkoot $A, B \in M_n(F)$, missä F on kunta. Matriisi A on *similaarinen* matriisin B:n kanssa, jos on olemassa sellainen kääntyvä matriisi $P \in M_n(F)$, että

$$A = PBP^{-1}.$$

Seuraavan lauseen perusteella voidaan myös sanoa, että A ja B ovat *similaariset*.

Lause 4.2. *Similaarisuus on ekvivalenssirelaatio.*

Todistus. Vrt. [1, s. 216]. Olkoot $A, B, C \in M_n(F)$, missä F on kunta. Koska I on kääntyvä ja $A = IAI^{-1}$, niin similaarisuus on refleksiivinen. Oletetaan seuraavaksi, että $A = PBP^{-1}$, missä P on kääntyvä $n \times n$-matriisi. Tällöin molemmilta puolilta kerrottaessa saadaan

$$B = P^{-1}A(P^{-1})^{-1}.$$

Luonnollisesti myös P^{-1} on kääntyvä matriisi, joten similaarisuus on symmetrinen.

Lopuksi osoitetaan vielä similaarisuuden transitiivisuus. Sitä varten oletetaan, että $A = PBP^{-1}$ ja $B = QCQ^{-1}$, missä P ja Q ovat kääntyviä. Seuraavassa päättelyssä hyödynnetään tietoa matriisikertolaskun liitännäisyydestä. Lisäksi tiedetään, että $(PQ)^{-1} = Q^{-1}P^{-1}$ ja siis kahden kääntyvän matriisin tulo on kääntyvä. Näin ollen

$$A = P(QCQ^{-1})P^{-1} = (PQ)C(Q^{-1}P^{-1}) = (PQ)C(PQ)^{-1}.$$

Similaarisuus täyttää kaikki kolme vaadittua ehtoa ja on siten ekvivalenssirelaatio. □

Määritelmä 4.3. Vrt. [9, s. 672]. Olkoot $A, B \in M_{mn}(R)$, missä R on yksiköllinen vaihdannainen rengas. Matriisin A sanotaan olevan *R-ekvivalentti* matriisin B kanssa, mikäli on olemassa sellaiset kääntyvät matriisit $P \in M_n(R)$ ja $Q \in M_m(R)$, että

$$A = QBP^{-1}.$$

Yhtä lailla voidaan sanoa, että matriisit A ja B ovat *R-ekvivalentit*.

Huomautus. Jos edellä esitetyssä määritelmässä pätee lisäksi, että P ja Q ovat *permutaatiomatriiseja* eli että ne on saatu identiteettimatriisista vaihtamalla sen rivejä tai sarakkeita keskenään, sanotaan, että A ja B ovat *permutaatioekvivalentit* (vrt. [10, s. 125]). Permutaatioekvivalenttius on siis tavallisen R-ekvivalenttiuden erikoistapaus. Tähän ekvivalenttiuden muotoon palataan luvussa 7. Määritelmän 4.3 yhtälössä voitaisiin hyvin käyttää matriisia P sen käänteismatriisin sijaan, sillä joka tapauksessa kumpikin on kääntyvä matriisi.

R-ekvivalenttius on samantapainen ominaisuus kuin similaarisuus. Se on nimittäin myös ekvivalenssirelaatio, mikä esitetään seuraavaksi lauseena.

Lause 4.4. *R-ekvivalenttius on ekvivalenssirelaatio.*

Todistus. Vrt. [3, s. 647]. Olkoot $A, B, C \in M_{mn}(R)$, missä R on yksiköllinen vaihdannainen rengas. Koska identiteettimatriisi on kääntyvä ja $A = I_m A I_n^{-1}$, voidaan ensin todeta, että R-ekvivalenttius on refleksiivinen. Oletetaan nyt, että $A = QBP^{-1}$, missä P ja Q ovat kääntyviä. Samoin niiden käänteismatriisit P^{-1} ja Q^{-1} ovat tietenkin kääntyviä. Kerrotaan yhtälö puolittain vasemmalta matriisilla Q^{-1} ja oikealta matriisilla $(P^{-1})^{-1}$, jolloin saamme uuden yhtälön

$$B = Q^{-1}A(P^{-1})^{-1} = Q^{-1}AP.$$

Täten R-ekvivalenttius on symmetrinen.

Oletetaan lopuksi, että $A = QBP^{-1}$ ja $B = SCR^{-1}$, missä $P, R \in M_n(R)$ ja $Q, S \in M_m(R)$ ovat kääntyviä. Vastaavin perusteluin kuin lauseen 4.2 transitiivisuuden todistuksessa

$$A = Q(SCR^{-1})P^{-1} = (QS)C(R^{-1}P^{-1}) = (QS)C(PR)^{-1}.$$

Lisäksi, kun matriisikertolaskun määritelmän nojalla tiedetään, että $QS \in M_m(R)$ ja $PR \in M_n(R)$, niin R-ekvivalenttius on transitiivinen. Loppujen lopuksi on saatu, että R-ekvivalenttius on ekvivalenssirelaatio. □

Apulause 4.5. Tarkastellaan kuntaa F. Olkoot $P \in M_n(F[x])$ ja $A \in M_n(F)$. Tällöin on olemassa sellaiset matriisit $Q_1, Q_2 \in M_n(F[x])$ ja $R_1, R_2 \in M_n(F)$, että

$$P = (xI - A)Q_1 + R_1, \quad P = Q_2(xI - A) + R_2.$$

Huomautus. Lauseen 3.2 perusteella $F[x]$ on euklidinen alue.

Todistus. Ks. [11, s. 201–202]. Jos $P \in M_n(F)$, niin valitsemalla $Q_1 = Q_2 = 0$ ja $R_1 = R_2 = P$ lauseen vaatimukset toteutuvat. Oletetaan siis, että $P \notin M_n(F)$. Tiedetään, että matriisi $P \in M_n(F[x])$ voidaan esittää muodossa

$$P = x^k C_k + x^{k-1}C_{k-1} + \cdots + C_0,$$

missä $C_j \in M_n(F)$ kaikilla $j \in \{0, 1, \ldots, k\}$. Tässä $k \geq 1$ ja $C_k \neq 0$. Tehdään seuraavat määritelmät:

$$Q_1 := x^{k-1}D_{k-1} + x^{k-2}D_{k-2} + \cdots + xD_1 + D_0,$$

$$Q_2 := x^{k-1}E_{k-1} + x^{k-2}E_{k-2} + \cdots + xE_1 + E_0,$$

missä

$$D_j = \sum_{m=0}^{k-1-j} A^m C_{m+1+j}, \quad j \in \{0, 1, \ldots, k-1\},$$

$$E_j = \sum_{m=0}^{k-1-j} C_{m+1+j} A^m, \quad j \in \{0, 1, \ldots, k-1\}.$$

Määritellään myös, että

$$R_1 := A^k C_k + A^{k-1} C_{k-1} + \cdots + AC_1 + C_0,$$

$$R_2 := C_k A^k + C_{k-1} A^{k-1} + \cdots + C_1 A + C_0.$$

Sijoittamalla edellä olevat merkinnät lauseen yhtälöihin $P = (xI - A)Q_1 + R_1$ ja $P = Q_2(xI - A) + R_2$ huomataan väitteen pätevän. □

Neliömatriisi $A \in M_n(F)$ on *skalaarimatriisi*, mikäli $A = cI$ jollakin $c \in F$. Tässä F:n oletetaan olevan kunta, ja I on $n \times n$-identiteettimatriisi. Skalaarimatriisien keskeinen ominaisuus on, että ne kommutoivat kaikkien samankokoisten matriisien kanssa. Tätä ominaisuutta hyödynnetään seuraavan lauseen todistuksessa.

Lause 4.6. *Olkoon F kunta. Tällöin neliömatriisit $A, B \in M_n(F)$ ovat similaariset, jos ja vain jos $xI - A, xI - B \in M_n(F[x])$ ovat $F[x]$-ekvivalentit.*

Todistus. Vrt. [11, s. 202–203]. Oletetaan ensin, että A ja B ovat similaariset. On siis olemassa sellainen kääntyvä matriisi $T \in M_n(F)$, että $A = TBT^{-1}$. Koska skalaarimatriisi xI kommutoi erityisesti matriisin T kanssa, saadaan

$$xI - A = (xI)TT^{-1} - A = T(xI)T^{-1} - A = T(xI)T^{-1} - TBT^{-1} = T(xI - B)T^{-1},$$

joten $xI - A$ ja $xI - B$ ovat $F[x]$-ekvivalentit.

Oletetaan sitten, että $xI - A$ ja $xI - B$ ovat $F[x]$-ekvivalentit. Määritelmän 4.3 mukaan on olemassa kääntyvät matriisit $P, S \in M_n(F[x])$, joille pätee

$$xI - A = S(xI - B)P^{-1}.$$

Täten kerrottaessa vasemmalta matriisilla S^{-1} päädytään yhtälöön

$$S^{-1}(xI - A) = (xI - B)P^{-1}.$$

Huomataan, että myös $P^{-1}, S^{-1} \in M_n(F[x])$. Apulauseen 4.5 nojalla on olemassa sellaiset matriisit $Q_1, Q_2 \in M_n(F[x])$ ja $R_1, R_2 \in M_n(F)$, että

$$S^{-1} = (xI - B)Q_1 + R_1, \quad P^{-1} = Q_2(xI - A) + R_2.$$

Sijoitetaan nämä kaksi esitysmuotoa edellä olevaan yhtälöön, jolloin

$$\big((xI - B)Q_1 + R_1\big)(xI - A) = (xI - B)\big(Q_2(xI - A) + R_2\big).$$

Tämä voidaan sieventää edelleen muotoon

$$(xI - B)(Q_1 - Q_2)(xI - A) = x(R_2 - R_1) + R_1A - BR_2.$$

Jos $Q_1 - Q_2 \neq 0$, niin yllä olevan yhtälön vasemman puolen aste on vähintään kaksi. Vastaavasti oikean puolen aste on enintään yksi. Tämä on ristiriitaista, joten voidaan päätellä, että $Q_1 - Q_2 = 0$ ja

$$x(R_2 - R_1) + R_1A - BR_2 = 0.$$

Tästä puolestaan seuraa, että $R_2 - R_1 = 0$ ja $R_1A - BR_2 = 0$. Näistä ensimmäisen perusteella $R_1 = R_2$. Sijoitetaan tämä tulos jälkimmäiseen yhtälöön ja saadaan $R_1A = BR_1$.

On vielä osoitettava, että $R_1 \in M_n(F)$ on kääntyvä. Apulauseen 4.5 perusteella on olemassa sellaiset matriisit $Q_3 \in M_n(F[x])$ ja $R_3 \in M_n(F)$, että

$$S = (xI - A)Q_3 + R_3.$$

Aikaisemmin todettiin, että $S^{-1} = (xI - B)Q_1 + R_1$, joten

$$\begin{aligned}
I &= S^{-1}S \\
&= \big((xI - B)Q_1 + R_1\big)\big((xI - A)Q_3 + R_3\big) \\
&= (xI - B)Q_1(xI - A)Q_3 + (xI - B)Q_1R_3 + R_1(xI - A)Q_3 + R_1R_3 \\
&= (xI - B)Q_1(xI - A)Q_3 + (xI - B)Q_1R_3 + R_1(xI)Q_3 - R_1AQ_3 + R_1R_3 \\
&= (xI - B)Q_1(xI - A)Q_3 + (xI - B)Q_1R_3 + (xI)R_1Q_3 - BR_1Q_3 + R_1R_3 \\
&= (xI - B)Q_1(xI - A)Q_3 + (xI - B)Q_1R_3 + (xI - B)R_1Q_3 + R_1R_3 \\
&= (xI - B)\big(Q_1(xI - A)Q_3 + Q_1R_3 + R_1Q_3\big) + R_1R_3.
\end{aligned}$$

Edellisessä päättelyketjussa hyödynnettiin matriisin xI kommutatiivisuutta toisen matriisin kanssa sekä aikaisemmin saatua tulosta $R_1A = BR_1$. Seuraavaksi voidaan todeta, että

$$I - R_1R_3 = (xI - B)\big(Q_1(xI - A)Q_3 + Q_1R_3 + R_1Q_3\big).$$

Nyt koska $I - R_1R_3 \in M_n(F)$, niin $Q_1(xI - A)Q_3 + Q_1R_3 + R_1Q_3 = 0$. Muuten yllä olevan yhtälön vasen puoli olisi vakioarvoinen matriisi, kun taas oikean puolen aste olisi vähintään yksi, mikä ei ole mahdollista. Siksi $R_1R_3 = I$, ja R_1 on kääntyvä. Yhtälöstä $R_1A = BR_1$ saadaan $B = R_1AR_1^{-1}$, joten B on similaarinen A:n kanssa. Lauseen 4.2 nojalla similaarisuus on kuitenkin symmetrinen ominaisuus, joten yhtä lailla A on similaarinen B:n kanssa. Väite pätee. □

4.2 Gaussin ekvivalenttius

Esitellään ensin merkintätapa, jota käytetään tutkielmassa tästä eteenpäin. Merkinnällä RIVI(i) tarkoitetaan kyseessä olevan matriisin A i. riviä. SARAKE(j) on vastaavasti A:n j. sarake. Näillä merkinnöillä on selvempää ilmaista matriiseille suoritettavia alkeisrivi- ja -sarakeoperaatioita, jotka esitelläänkin seuraavaksi heti alaluvun alkuun. Sen jälkeen käsitellään alkeisoperaatioita matriisikertolaskuna ja lopuksi määritellään Gaussin ekvivalenttius.

Määritelmä 4.7. Vrt. [9, s. 675]. Olkoon R yksiköllinen vaihdannainen rengas. Matriisiin $A \in M_{mn}(R)$ voidaan käyttää kolmea *alkeisrivioperaatiota*:

1) Kerrotaan RIVI(i) yksiköllä $u \in R$.

2) Korvataan RIVI(i) alkiolla RIVI(i)+c·RIVI(j), missä $i \neq j$ ja $c \in R$.

3) Vaihdetaan RIVI(i) ja RIVI(j) keskenään.

Vastaavasti määritellään *alkeissarakeoperaatiot*.

Huomautus. Joskus määritelmän 4.7 ensimmäinen kohta saatetaan muotoilla yksiköllä jakamiseksi (ks. esimerkiksi [1, s. 225]).

Periaatteessa kaksi alkeisoperaatiota riittää, sillä rivien (tai sarakkeiden) vaihtaminen keskenään voidaan toteuttaa kahden muun operaation avulla:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \overset{2.}{\to} \begin{pmatrix} a-c & b-d \\ c & d \end{pmatrix} \overset{2.}{\to} \begin{pmatrix} a-c & b-d \\ a & b \end{pmatrix} \overset{2.}{\to} \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \overset{1.}{\to} \begin{pmatrix} c & d \\ a & b \end{pmatrix}.$$

Jokainen edellä esitetyistä operaatioista vastaa kertomista kääntyvällä neliömatriisilla. Jos tarkastellaan esimerkiksi 3×3-matriisia A, kertominen vasemmalta matriisilla

$$L_1 = \begin{pmatrix} u & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

eli $L_1 A$ tuottaa matriisin, jossa A:n ensimmäinen rivi on kerrottu yksiköllä u. Vastaavasti ensimmäisen sarakkeen saa kerrottua yksiköllä matriisikertolaskulla AL_1. Luonnollisesti ”siirtämällä” yksikköä u lävistäjällä pystytään kertomaan muita kuin ensimmäisiä rivejä ja sarakkeita.

Jatketaan samaa esimerkinomaista tarkastelua. Yksi tapa suorittaa määritelmän 4.7 toinen alkeisrivioperaatio on kertoa alkuperäinen matriisi A vasemmalta matriisilla

$$L_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ c & 0 & 1 \end{pmatrix},$$

jolloin A:n kolmanteen riviin lisätään ensimmäinen rivi kerrottuna alkiolla c. Jos sen sijaan kolmanteen sarakkeeseen halutaan lisätä ensimmäinen sarake c:llä kerrottuna, lasketaan matriisikertolasku AL_2', missä

$$L_2' = \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Viimeisenä tarkastellaan vielä, miten matriisin A rivit (tai sarakkeet) saadaan vaihdettua keskenään. Ratkaisuna on permutaatiomatriisi. Jos permutaatiomatriisi on muotoa

$$L_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

niin L_3A tuottaa uuden matriisin, jossa alkuperäisen A:n ensimmäinen ja toinen rivi on vaihdettu keskenään. Vastaavasti laskutoimitus AL_3 vaihtaa A:n ensimmäisen ja toisen sarakkeen keskenään.

Määritelmä 4.8. Ks. [9, s. 676]. *Alkeismatriisi* on matriisi, joka saadaan identiteettimatriisista I suorittamalla sille yksi alkeisrivioperaatio. Alkeissarakeoperaatioiden käyttäminen saa aikaan saman alkeismatriisien joukon.

Esimerkki 4.1. Edellä esitetyt matriisit L_1, L_2, L_2' ja L_3 ovat alkeismatriiseja.

On siis olemassa kolmen tyyppisiä alkeismatriiseja riippuen siitä, mikä kolmesta alkeisoperaatiosta on suoritettu identiteettimatriisille. Jokainen alkeismatriisi on kääntyvä, ja sen käänteismatriisi on samantyyppinen alkeismatriisi. Tämän seurauksena alkeismatriisien tulo on aina kääntyvä.

Määritelmä 4.9. Ks. [9, s. 676]. Olkoon R yksiköllinen vaihdannainen rengas. Tällöin matriisi Γ on *Gaussin ekvivalentti* matriisin Γ' kanssa, mikäli on olemassa jono sellaisia alkeisrivi- ja -sarakeoperaatioita, että

$$\Gamma = \Gamma_0 \to \Gamma_1 \to \cdots \to \Gamma_r = \Gamma'.$$

Tässä matriisien Γ ja Γ' alkiot kuuluvat renkaaseen R. Voidaan myös sanoa, että matriisit Γ ja Γ' ovat *Gaussin ekvivalentit*. Nuolimerkinnällä tarkoitetaan jatkossa siis alkeisrivi- tai -sarakeoperaatiota.

Kuten aiemmin määritellyt käsitteet similaarisuus ja R-ekvivalenttius, myös Gaussin ekvivalenttius on ekvivalenssirelaatio. Näihin käsitteisiin palataan vielä tulevissa luvuissa. Päätetään tämä luku kuitenkin esimerkkiin Gaussin ekvivalenteista matriiseista.

Esimerkki 4.2. Tarkastellaan kokonaislukujen rengasta $\mathbb{Z}$. Koska

$$\Gamma = \begin{pmatrix} 3 & 0 & 5 \\ 1 & 4 & 9 \\ 7 & 2 & 6 \end{pmatrix} \overset{3.}{\to} \begin{pmatrix} 1 & 4 & 9 \\ 3 & 0 & 5 \\ 7 & 2 & 6 \end{pmatrix} \overset{1.}{\to} \begin{pmatrix} 1 & 4 & 9 \\ -3 & 0 & -5 \\ 7 & 2 & 6 \end{pmatrix} \overset{2.}{\to} \begin{pmatrix} 1 & 3 & 9 \\ -3 & 3 & -5 \\ 7 & -5 & 6 \end{pmatrix} = \Gamma',$$

matriisit Γ ja Γ' ovat Gaussin ekvivalentit. Ensimmäisessä vaiheessa vaihdetaan RIVI(1) ja RIVI(2) keskenään. Seuraavaksi kerrotaan RIVI(2) yksiköllä -1. Huomaa, että kokonaislukujen renkaassa yksiköitä ovat vain ± 1. Lopuksi SARAKE(2) korvataan summalla SARAKE(2)+$(-1)\cdot$SARAKE(1). Matriisit Γ ja Γ' voidaan osoittaa Gaussin ekvivalenteiksi yhtä hyvin myös toisenlaisella alkeisoperaatioiden jonolla. Nämä jonot eivät siis ole yksikäsitteisiä.

5 Päälause

Nyt ollaan valmiita todistamaan Henry John Stephen Smithin vuonna 1861 löytämä tulos, joka kantaa nimeä Smithin normaalimuoto. Sitä voidaan pitää tämän tutkielman keskeisimpänä lauseena.

Lause 5.1. (Smithin normaalimuoto). *Olkoon* Γ *nollamatriisista eroava* $n \times t$*-matriisi, jonka alkiot kuuluvat euklidiseen alueeseen* E*. Tällöin* Γ *on Gaussin ekvivalentti muotoa*

$$\begin{pmatrix} \Sigma & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$$

olevan matriisin kanssa, missä $\Sigma = diag(\sigma_1, \sigma_2, \ldots, \sigma_q)$ *ja nollasta poikkeaville lävistäjäalkioille* $\sigma_1, \sigma_2, \ldots, \sigma_q \in E$ *pätee ehto* $\sigma_1 \mid \sigma_2 \mid \cdots \mid \sigma_q$.

Huomautus. Lauseessa esiintyvä matriisi voi olla myös ilman alhaalla tai oikealla esitettyjä nollalohkoja $\mathbf{0}$. Esimerkkinä tästä toimii kääntyvä matriisi Γ. Alkeisrivi- ja -sarakeoperaatiot säilyttävät Γ:n kanssa Gaussin ekvivalentin matriisin kääntyvänä. Tämä puolestaan tarkoittaa sitä, ettei Smithin normaalimuoto voi sisältää nollarivejä tai -sarakkeita. Muuten matriisi ei olisi enää alkeisoperaatioiden jälkeen kääntyvä. Tässä tapauksessa Γ on siis Gaussin ekvivalentti lävistäjämatriisin Σ kanssa.

Todistus. Vrt. [9, s. 676–677]. Todistetaan väite induktiolla Γ:n rivien lukumäärän $n \geq 1$ suhteen. Merkitään nollasta poikkeavan alkion $\sigma \in E$ astetta $\partial(\sigma)$. Olkoon $\sigma_1 \in E$ pieniasteisin alkio kaikkien matriisin Γ kanssa Gaussin ekvivalenttien matriisien sisältämien nollasta eroavien alkioiden joukossa. Olkoon Δ puolestaan matriisi, joka on Gaussin ekvivalentti matriisin Γ kanssa ja jolla on alkionaan σ_1. Vaihtamalla matriisin Δ rivejä (tai vastaavasti sarakkeita) keskenään on aina mahdollista muodostaa matriisin Γ kanssa Gaussin ekvivalentti matriisi, jolla on alkiona σ_1 paikassa $(1, 1)$. Siksi voidaan olettaa, että σ_1 sijaitsee matriisin Δ paikassa $(1, 1)$.

Osoitetaan ensin, että $\sigma_1 \mid \eta_{1j}$ kaikilla matriisin Δ ensimmäisen rivin alkioilla η_{1j}. Jos näin ei olisi, täytyy ensinnäkin olla olemassa sellainen sarake j, että $j \neq 1$ ja siis $\sigma_1 \nmid \eta_{1j}$. Koska tarkastellaan euklidista aluetta, jakoalgoritmi on voimassa. Täten määritelmän 3.1 mukaan $\eta_{1j} = \kappa\sigma_1 + \rho$ joillakin $\kappa, \rho \in E$ ja joko $\rho = 0$ tai $\partial(\rho) < \partial(\sigma_1)$. Koska $\sigma_1 \nmid \eta_{1j}$, on oltava $\partial(\rho) < \partial(\sigma_1)$. Kun korvataan SARAKE($j$) summalla SARAKE($j$)+($-\kappa$)SARAKE(1), saadaan uusi matriisi Δ', missä on alkiona ρ. Matriisi Δ' on Gaussin ekvivalentti matriisin Γ kanssa, ja se sisältää alkion $\rho \neq 0$, jonka aste on pienempi kuin σ_1:n aste. Päädytään ristiriitaan. Siksi σ_1 jakaa jokaisen samalla rivillä olevan alkion. Samaan tapaan voidaan osoittaa, että σ_1 jakaa myös jokaisen samalla sarakkeella olevan alkion.

Palataan tarkastelemaan matriisia Δ, joka on siis Gaussin ekvivalentti Γ:n kanssa ja joka sisältää alkionaan σ_1:n paikassa $(1, 1)$. Osoitetaan seuraavaksi, että σ_1 jakaa jokaisen matriisin Δ alkioista. Olkoon a sellainen alkio, että se ei sijaitse samalla rivillä tai sarakkeella σ_1:n kanssa. Keskitytään nyt matriisin Δ alimatriisiin

$$\begin{pmatrix} \sigma_1 & b \\ c & a \end{pmatrix},$$

missä $b = u\sigma_1$ ja $c = v\sigma_1$ joillakin $u, v \in E$. Jos korvataan alimatriisin toinen sarake summalla SARAKE(2)+$(1-u)$SARAKE(1), päästään muotoon

$$\begin{pmatrix} \sigma_1 & b + (1-u)\sigma_1 \\ c & a + (1-u)c \end{pmatrix} = \begin{pmatrix} \sigma_1 & \sigma_1 \\ c & a + (1-u)c \end{pmatrix}.$$

Kuten äsken todettiin, σ_1 jakaa saman sarakkeen alkiot. Siksi $\sigma_1 \mid a + (1-u)c$. Koska $\sigma_1 \mid c$, voidaan päätellä, että $\sigma_1 \mid a$. Täten σ_1 on Δ:n alkio, joka jakaa kaikki matriisin Δ alkiot.

Olkoon η_{1r} matriisin Δ jokin σ_1:stä eroava ensimmäisen rivin alkio. Täten se voidaan esittää muodossa $\eta_{1r} = \kappa_r\sigma_1$, missä $\kappa_r \in E$. Korvataan SARAKE(r) summalla SARAKE(r)+$(-\kappa_r)$SARAKE(1), jolloin saadussa matriisissa on alkiona nolla paikassa $(1, r)$. Täten tämän Gaussin ekvivalentin matriisin paikassa $(1, 1)$ on σ_1, ja muut alkiot ensimmäisellä rivillä ovat nollia. Näin on itse asiassa osoitettu, että nollamatriisista eroava $1 \times t$-matriisi on Gaussin ekvivalentti matriisin

$$\begin{pmatrix} \sigma_1 & 0 & \dots & 0 \end{pmatrix}$$

kanssa. Väite siis pätee, kun matriisissa Γ on vain yksi rivi. Alkeisrivioperaatioita vastaavasti käyttämällä voidaan muodostaa matriisin Γ kanssa Gaussin ekvivalentti matriisi, jossa lisäksi kaikki ensimmäisen sarakkeen alkiot σ_1:ä lukuunottamatta ovat nollia.

Oletetaan, että väite pätee, kun matriisin Γ rivien lukumäärä on $n = k-1$ ja osoitetaan, että väite pätee myös, kun rivejä on $n = k$ kappaletta. Edellä esitetyn nojalla Γ on Gaussin ekvivalentti sellaisen matriisin kanssa, että kaikki muut alkiot kuin σ_1 ensimmäisellä rivillä sekä sarakkeella ovat nollia. Siis Γ on Gaussin ekvivalentti matriisin

$$\begin{pmatrix} \sigma_1 & \mathbf{0} \\ \mathbf{0} & \Omega \end{pmatrix}.$$

kanssa, missä on $n = k$ riviä. Induktio-oletuksen nojalla matriisi Ω on Gaussin ekvivalentti puolestaan matriisin

$$\begin{pmatrix} \Sigma' & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$$

kanssa. Tässä $\Sigma' = \operatorname{diag}(\sigma_2, \sigma_3, \dots, \sigma_q)$ ja $\sigma_2 \mid \sigma_3 \mid \cdots \mid \sigma_q$ sekä rivejä on yhteensä $n = k-1$. Näin ollen Γ on Gaussin ekvivalentti matriisin

$$\begin{pmatrix} \sigma_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \Sigma' & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \Sigma & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$$

kanssa. Saatu matriisi täyttää samat oletukset kuin Δ. Siksi σ_1 jakaa jokaisen tämän matriisin alkioista ja etenkin $\sigma_1 \mid \sigma_2$. □

Määritelmä 5.2. Ks. [9, s. 677]. Lauseessa 5.1 esiintyvää matriisia

$$\begin{pmatrix} \Sigma & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$$

kutsutaan Γ:n *Smithin normaalimuodoksi*.

Esimerkki 5.1. Saatetaan $\mathbb{R}[x]$-kertoiminen matriisi

$$\begin{pmatrix} 2x & 2x-1 & x+3 \\ -2x^2-x & -2x^2 & -x^2-3x \\ 2x^2+4x & 2x^2+3x-2 & x^2+6x+7 \end{pmatrix}$$

sen Smithin normaalimuotoon (tehtävänanto ks. [2, s. 331]). On olemassa lukuisia eri tapoja päätyä samaan lopputulokseen. Tässä esitetään yksi niistä. Lähes kaikissa vaiheissa käytetään määritelmän 4.7 toisen tyypin alkeisoperaatioita.

Aloitetaan korvaamalla SARAKE(1) summalla SARAKE(1) $+(-1)$SARAKE(2):

$$\begin{pmatrix} 1 & 2x-1 & x+3 \\ -x & -2x^2 & -x^2-3x \\ x+2 & 2x^2+3x-2 & x^2+6x+7 \end{pmatrix}.$$

Seuraavaksi muutetaan toinen rivi muotoon RIVI(2) + RIVI(3), jolloin saadaan

$$\begin{pmatrix} 1 & 2x-1 & x+3 \\ 2 & 3x-2 & 3x+7 \\ x+2 & 2x^2+3x-2 & x^2+6x+7 \end{pmatrix}.$$

Jatketaan toisen rivin muokkaamista ja korvataan se summalla RIVI(2) $+(-2)$RIVI(1), jolloin matriisi tulee muotoon

$$\begin{pmatrix} 1 & 2x-1 & x+3 \\ 0 & -x & x+1 \\ x+2 & 2x^2+3x-2 & x^2+6x+7 \end{pmatrix}.$$

Matriisin paikkaan $(3,1)$ halutaan seuraavaksi nolla, joten suoritetaan 3. riville ensin korvaava alkeisrivioperaatio RIVI(3) $+(-x-2)$RIVI(1) ja jatketaan vielä korvaamalla RIVI(1) summalla RIVI(1) $+2\cdot$RIVI(2):

$$\begin{pmatrix} 1 & 2x-1 & x+3 \\ 0 & -x & x+1 \\ 0 & 0 & x+1 \end{pmatrix} \to \begin{pmatrix} 1 & -1 & 3x+5 \\ 0 & -x & x+1 \\ 0 & 0 & x+1 \end{pmatrix}.$$

Seuraavat operaatiot ovat alkeissarakeoperaatioita. Ensin toinen sarake muutetaan summaksi SARAKE(2) + SARAKE(1), sitten muokataan SARAKE(3) summaksi SARAKE(3) $+(-3x-5)$SARAKE(1) ja lopuksi jälleen SARAKE(2) summaksi SARAKE(2) + SARAKE(3). Tällöin päästään muotoon

$$\begin{pmatrix} 1 & 0 & 3x+5 \\ 0 & -x & x+1 \\ 0 & 0 & x+1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x & x+1 \\ 0 & 0 & x+1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x+1 \\ 0 & x+1 & x+1 \end{pmatrix}.$$

Tämän jälkeen korvataan RIVI(3) summalla RIVI(3) $+(-x-1)$RIVI(2) ja SARAKE(3) summalla SARAKE(3) $+(-x-1)$SARAKE(2):

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x+1 \\ 0 & 0 & -x^2-x \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -x^2-x \end{pmatrix}.$$

Tehtävän voisi jättää tähän, mutta kerrotaan vielä RIVI(3) yksiköllä -1, jolloin matriisi saadaan loppujen lopuksi Smithin normaalimuotoon

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^2 + x \end{pmatrix}.$$

Tässä tapauksessa on helppo huomata, että lävistäjäalkiot todella jakavat toisensa.

Smithin normaalimuoto onkin yksiköllä kertomista vaille yksikäsitteinen, mikä seuraa myöhemmin esitettävästä lauseesta 6.4. Matriisin Smithin normaalimuoto on kuitenkin tapana laittaa muotoon, jossa lävistäjällä on ainoastaan pääpolynomeja mahdollisten nolla-alkioiden lisäksi. Tämä on tosin yleisesti mahdollista vain matriisin sisältämien polynomien kertoimien kuuluessa johonkin kuntaan. Tällöin polynomirengas on nimittäin lauseen 3.2 perusteella euklidinen alue. Esimerkiksi kokonaislukukertoimisesta polynomista $2x + 1$ ei saa kokonaislukukertoimista pääpolynomia.

Mainittakoon myös, että Smithin normaalimuodossa lävistäjällä on alkuperäisen matriisin asteen verran alkioita, joilla on nollasta poikkeava vakiotermi. Mikäli vaatimuksena on, että kuntakertoimisia polynomeja sisältävän matriisin lävistäjän nollasta eroavat alkiot ovat pääpolynomeja, Smithin normaalimuoto on siis yksikäsitteinen.

Huomautus. Joskus kirjallisuudessa mainitaan erikseen Smithin normaalimuodon erikoistapaus, jossa tarkasteltava matriisi on Gaussin ekvivalentti matriisin

$$\begin{pmatrix} I_q & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$$

kanssa. Tässä I_q on identiteettimatriisi, ja matriisin aste on q. Tässä erikoistapauksessa matriisin alkioiden on kuitenkin kuuluttava kuntaan euklidisen alueen sijaan (ks. [1, s. 167–168, 227]).

Huomautus. Matriisia alkeisoperaatioilla muokattaessa saattaa päätyä lävistäjämatriisimuotoon $\operatorname{diag}(\sigma_1, \sigma_2, \ldots, \sigma_q)$, missä on kuitenkin jokin lävistäjäalkio σ_i, jolle pätee $\sigma_i \nmid \sigma_{i+1}$. Tällöin täytyy jatkaa matriisin muokkaamista, kunnes päästään haluttuun muotoon.

Apulause 5.3. Olkoon E euklidinen alue. Jos neliömatriisi $\Gamma \in M_n(E)$ on kääntyvä, se voidaan esittää alkeismatriisien tulona.

Todistus. Vrt. [9, s. 677–678]. Oletetaan, että $\Gamma \in M_n(E)$ on kääntyvä. Lauseen 5.1 yhteydessä olevan huomautuksen nojalla tiedetään, että Γ on Gaussin ekvivalentti lävistäjämatriisin Σ kanssa. On siis olemassa sellaiset alkeismatriisien tulosta koostuvat matriisit P ja Q, että

$$P\Gamma Q = \Sigma = \operatorname{diag}(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Kun tämä yhtälö kerrotaan vasemmalta P^{-1}:llä ja oikealta Q^{-1}:llä, seurauksena on, että $\Gamma = P^{-1}\Sigma Q^{-1}$. Koska alkeismatriisin käänteismatriisi on aina alkeismatriisi, P^{-1} ja Q^{-1} ovat myös alkeismatriisien tuloja.

Koska Σ on lävistäjämatriisi, jonka lävistäjällä ei ole nollia, se on kääntyvä. Lisäksi E on euklidisena alueena yksiköllinen vaihdannainen rengas, joten lauseen 2.20 perusteella Σ:n determinantti $\det(\Sigma) = \sigma_1\sigma_2\cdots\sigma_n$ on yksikkö E:ssä. On siis olemassa jokin sellainen $a \in E$, että

$$(\sigma_1\sigma_2\cdots\sigma_n)\cdot a = 1.$$

Kertolaskun liitännäisyyttä hyödyntämällä saadaan vastaavasti, että

$$\sigma_1 \cdot (\sigma_2\cdots\sigma_n a) = 1,$$

joten myös σ_1 on euklidisen alueen E yksikkö. E on vaihdannainen rengas, ja täten voidaan lisäksi päätellä, että

$$\begin{aligned}\sigma_2 \cdot (\sigma_1\sigma_3\cdots\sigma_n a) &= (\sigma_2\sigma_1)(\sigma_3\cdots\sigma_n a)\\ &= (\sigma_1\sigma_2)(\sigma_3\cdots\sigma_n a)\\ &= (\sigma_1\sigma_2\cdots\sigma_n)\cdot a\\ &= 1.\end{aligned}$$

Näin ollen σ_2 on yksikkö E:ssä. Vastaavasti voidaan päätellä, että σ_i on yksikkö kaikilla $i \in \{1, 2, \ldots, n\}$. Täten Σ koostuu sellaisten alkeismatriisien tulosta, että ne on saatu kertomalla RIVI(i) yksiköllä σ_i. Näitä alkeismatriiseja on n kappaletta. Kokonaisuudessaan siis Γ voidaan esittää alkeismatriisien tulona. □

Lause 5.4. *Olkoon E euklidinen alue. Tällöin kaksi matriisia $\Gamma, \Gamma' \in M_{nt}(E)$ on E-ekvivalentit, jos ja vain jos ne ovat Gaussin ekvivalentit.*

Todistus. Vrt. [9, s. 678]. Oletetaan ensin, että Γ ja Γ' ovat E-ekvivalentit. Tällöin määritelmän mukaan on olemassa kääntyvät matriisit P ja Q, joille pätee

$$\Gamma = Q\Gamma' P^{-1}.$$

Tietenkin myös P^{-1} on kääntyvä. Apulauseen 5.3 perusteella matriisit Q ja P^{-1} voidaan esittää alkeismatriisien tuloina. Tämä on sama asia kuin että Γ ja Γ' ovat Gaussin ekvivalentit.

Oletetaan sitten, että Γ ja Γ' ovat Gaussin ekvivalentit. Nyt $\Gamma = P\Gamma' Q$, missä P ja Q ovat alkeismatriisien tuloja. Alkeismatriisit ovat kääntyviä, ja kääntyvien matriisien tulo on aina kääntyvä, joten P ja Q ovat kääntyviä. Tämän perusteella Γ ja Γ' ovat E-ekvivalentit. Ei ole olennaista, käytetäänkö merkinnöissä käänteismatriisia vai ei. Huomaa, että jälkimmäinen suunta pätee kaikille yksiköllisille vaihdannaisille renkaille ilman oletusta euklidisesta alueesta. □

6 Invariantit tekijät ja alkeisjakajat

Saattamalla matriisin Smithin normaalimuotoon saadaan selville sen invariantit tekijät ja alkeisjakajat. Aloitetaan tämä luku käsittelemällä invariantteja tekijöitä.

6.1 Invariantit tekijät

Ensin on luonnollista määritellä, mitä invarianteilla tekijöillä (engl. *invariant factors*) tarkoitetaan. Tässä hyödynnetään yksinkertaista muun muassa Bakerin ja Porteousin käyttämää määritelmää. Rotman sen sijaan määrittelee invariantit tekijät niin sanotun *rationaalisen kanonisen muodon* avulla, jota ei kuitenkaan käsitellä tässä tutkielmassa.

Määritelmä 6.1. Vrt. [1, s. 227]. Tarkastellaan $n \times t$-matriisin A Smithin normaalimuotoa

$$\begin{pmatrix} \sigma_1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \sigma_2 & 0 & 0 & 0 & & 0 \\ 0 & 0 & \ddots & 0 & 0 & & 0 \\ 0 & 0 & 0 & \sigma_q & 0 & & 0 \\ 0 & 0 & 0 & 0 & 0 & & 0 \\ \vdots & & & & & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Alkioita $\sigma_1, \sigma_2, \dots, \sigma_q \neq 0$ kutsutaan A:n *invarianteiksi tekijöiksi*. Määritellään, että nollamatriisilla ei ole invariantteja tekijöitä.

Huomautus. Joissakin lähteissä (ks. esimerkiksi [4, s. 558]) ylläolevia nollasta poikkeavia alkioita sanotaan matriisin *A Smithin invarianteiksi*.

Esimerkki 6.1. Jatketaan esimerkkiä 5.1. Siinä $\mathbb{R}[x]$-kertoimisen matriisin

$$\begin{pmatrix} 2x & 2x-1 & x+3 \\ -2x^2-x & -2x^2 & -x^2-3x \\ 2x^2+4x & 2x^2+3x-2 & x^2+6x+7 \end{pmatrix}$$

Smithin normaalimuodoksi saatiin

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^2+x \end{pmatrix}.$$

Koska käsitellyn matriisin aste on 3, sillä on myös kolme invarianttia tekijää: 1, 1 ja x^2+x. Tässä 1 on *kaksinkertainen invariantti tekijä*. Huomaa, että joissakin teoksissa yksiköitä ei lueta invarianteiksi tekijöiksi. Tässä tapauksessa löydettäisiin siis yksi ainoa invariantti tekijä $x^2 + x$.

Määritelmä 6.2. Ks. [9, s. 100]. Yksiköllisen vaihdannaisen renkaan R alkiot a ja b ovat *liittoalkioita* (engl. *associates*), jos on olemassa sellainen yksikkö $u \in R$, että $b = ua$.

Apulause 6.3. Olkoon R kokonaisalue, ja olkoot $a, b \in R$. Tällöin $a \mid b$ ja $b \mid a$, jos ja vain jos a ja b ovat liittoalkioita keskenään.

Todistus. Ks. [9, s. 100]. Oletetaan ensin, että $a \mid b$ ja $b \mid a$. On siis olemassa sellaiset alkiot $r, s \in R$, että $b = ra$ ja $a = sb$. Näin ollen $b = rsb$. Nyt jos $b = 0$, niin myös $a = s0 = 0$, jolloin väite pätee. Tarkastellaan seuraavaksi tapausta $b \neq 0$. Koska tarkastelemme kokonaisaluetta, supistussääntö on voimassa. Siksi $rs = 1$, ja r ja s ovat yksiköitä. Tästä seuraa, että a ja b ovat liittoalkioita keskenään.

Oletetaan sitten, että a ja b ovat liittoalkioita. Määritelmän nojalla on olemassa yksikkö $u \in R$, jolle pätee $b = ua$. Täten siis $a \mid b$. Koska u on yksikkö R:ssä, niin on olemassa sellainen $u^{-1} \in R$, että $u^{-1}u = 1$. Nyt saadaan $a = u^{-1}b$, joten myös $b \mid a$. □

Lause 6.4. *Olkoon $\Gamma \in M_{mn}(E)$, missä E on euklidinen alue. Merkitään lisäksi, että $\Sigma = diag(\sigma_1, \sigma_2, \ldots, \sigma_q)$ on matriisin Γ Smithin normaalimuodon lävistäjäosa. Määritellään σ_i:t rekursiivisesti: $d_0(\Gamma) = 1$, ja kaikilla $1 \leq i \leq \min\{m, n\}$*

$d_i(\Gamma)$ tarkoittaa kaikkien matriisin Γ $i \times i$-minorien suurinta yhteistä tekijää.

Tällöin kaikille $1 \leq i \leq \min\{m, n\}$ pätee

$$\sigma_i \sim \frac{d_i(\Gamma)}{d_{i-1}(\Gamma)}.$$

Tässä merkinnällä $a \sim b$ tarkoitetaan, että a ja b ovat liittoalkioita euklidisessa alueessa E.

Todistus. Vrt. [9, s. 680]. Osoitetaan, että jos Γ ja Γ' ovat Gaussin ekvivalentit, niin

$$d_i(\Gamma) \sim d_i(\Gamma')$$

kaikilla $1 \leq i \leq \min\{m, n\}$. Tämä riittää lauseen todistamiseksi, sillä jos Γ' on matriisin Γ Smithin normaalimuoto, missä lävistäjäosa on $\mathrm{diag}(\sigma_1, \sigma_2, \ldots, \sigma_q)$, niin $d_i(\Gamma') = \sigma_1\sigma_2 \cdots \sigma_i$. Näin ollen

$$\sigma_i = \frac{d_i(\Gamma')}{d_{i-1}(\Gamma')} \sim \frac{d_i(\Gamma)}{d_{i-1}(\Gamma)}.$$

Riittää osoittaa, että $d_i(\Gamma) \sim d_i(L\Gamma)$ ja $d_i(\Gamma) \sim d_i(\Gamma L)$, missä L on mikä tahansa alkeismatriisi. Ensimmäinen näistä käsittää alkeisrivioperaatiot ja jälkimmäinen alkeissarakeoperaatiot. Halutaan siis seuraavaksi todistaa, että alkeisrivi- tai -sarakeoperaation suorittaminen matriisiin Γ säilyttää minorien suurimpien yhteisten tekijöiden liittoalkio-ominaisuuden Γ:n ja saadun matriisin välillä.

Tästä voidaan edetä vielä yksinkertaisempaan muotoon. Itse asiassa riittää osoittaa, että $d_i(L\Gamma) \sim d_i(\Gamma)$, koska

$$d_i(L\Gamma) = d_i((L\Gamma)^\top) = d_i(\Gamma^\top L^\top).$$

Tässä matriisin $\Gamma^\top$ $i \times i$-alimatriisit ovat matriisin Γ $i \times i$-alimatriisien transpooseja. Lisäksi $L^\top$ on alkeismatriisi, ja jokaisen neliömatriisin transpoosin determinantti on yhtä suuri kuin itse matriisin determinantti. Sarakeoperaatiotapaus voidaan siis jättää käsittelemättä symmetriasyistä.

Tehdään viimeinen yksinkertaistus todistettavalle väitteelle. Määritelmän 4.7 jälkeen havaittiin, että kahden rivin vaihtaminen keskenään on mahdollista toteuttaa kahden muun alkeisoperaation avulla. Siksi riittää tarkistaa tapaukset, joissa alkeismatriisi L on tyyppiä 1) tai 2).

Oletetaan ensin, että L on tyyppiä 1). Jos kerrotaan matriisin Γ RIVI(l) yksiköllä u, joko $i \times i$-alimatriisi säilyy muuttumattomana tai yksi sen riveistä kerrotaan u:lla. Mikäli alimatriisissa ei tapahdu muutoksia, minori pysyy tietenkin myös ennallaan. Jos sen sijaan yksi rivi kerrotaan yksiköllä u, myös minori muuttuu tämän yksikön verran. Siksi matriisin $L\Gamma$ jokainen $i \times i$-minori on liittoalkio matriisin Γ vastaavan $i \times i$-minorin kanssa. Aiemmin esitettyä merkintää käyttäen siis $d_i(L\Gamma) \sim d_i(\Gamma)$.

Oletetaan lopuksi, että L on tyyppiä 2). Mikäli alkeismatriisia L käyttämällä korvataan matriisissa Γ RIVI(l) summalla RIVI(l)+r·RIVI(j), ainoastaan RIVI(l) muuttuu. Nyt tämä rivi joko kuuluu Γ:n $i \times i$-alimatriisiin tai ei kuulu. Jälkimmäisessä tapauksessa alimatriisi ei muutu mitenkään, joten myös minori pysyy samana. Tarkastellaankin seuraavaksi tapausta, jossa alimatriisin yksi rivi muuttuu. Tällöin $i \times i$-alimatriisin minori tulee muotoon $m + rm'$, missä m ja m' ovat Γ:n $i \times i$-minoreita. Koska suurimman yhteisen tekijän määritelmän nojalla $d_i(\Gamma) \mid m$ ja $d_i(\Gamma) \mid m'$, niin $d_i(\Gamma) \mid m + rm'$. Toisin sanoen $d_i(\Gamma) \mid d_i(L\Gamma)$. Tiedetään, että matriisi L^{-1} on myös tyypin 2) alkeismatriisi, joten saadaan, että $d_i(L^{-1}(L\Gamma)) \mid d_i(L\Gamma)$. Tässä tietenkin $L^{-1}(L\Gamma) = \Gamma$. Koska neliömatriiseille A ja B pätee $\det(AB) = \det(A)\det(B)$, yhtälön $L^{-1}(L\Gamma) = \Gamma$ perusteella päädytään tulokseen $d_i(L^{-1})d_i(L\Gamma) = d_i(\Gamma)$. Tästä päätellään, että $d_i(L\Gamma) \mid d_i(\Gamma)$. On siis saatu, että $d_i(\Gamma)$ ja $d_i(L\Gamma)$ jakavat toisensa. Koska E on euklidisena alueena kokonaisalue, voidaan käyttää apulausetta 6.3. Sen perusteella $d_i(L\Gamma) \sim d_i(\Gamma)$. □

Huomautus. Lauseessa 6.4 esiintyneitä suurimpia yhteisiä tekijöitä $d_i(\Gamma)$ kutsutaan matriisin Γ *determinanttisiksi jakajiksi* (engl. *determinantal divisors*) (ks. [4, s. 558]).

Lause 6.4 osoittaa, että invariantit tekijät ja näin ollen Smithin normaalimuoto ovat yksiköllä kertomista vaille yksikäsitteiset. Kukin invariantti tekijä voidaan määrittää kaavalla

$$\sigma_i = \frac{d_i(\Gamma)}{d_{i-1}(\Gamma)},$$

mutta on muistettava, että yhtä lailla millä tahansa yksiköllä u kerrottu osamäärä

$$\sigma_i' = u \cdot \frac{d_i(\Gamma)}{d_{i-1}(\Gamma)}$$

kelpaa i. invariantiksi tekijäksi. Siksi esimerkiksi kokonaislukujen renkaassa Smithin normaalimuodot

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \text{ ja } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

ovat erisuuret. Sen sijaan rationaalilukujen joukossa luku $\frac{3}{2}$ on yksikkö. Kun sillä kerrotaan edellä esitetyn ensimmäisen Smithin normaalimuodon kolmas invariantti tekijä, havaitaan, että nämä kaksi Smithin normaalimuotoa ovat itse asiassa samat. Määritellään seuraavaksi käsite, joka on hyödyllinen konkreettisessa invarianttien tekijöiden määrittämisessä.

Määritelmä 6.5. Vrt. [9, s. 132]. Olkoon F kunta. Tällöin tarkasteltavien polynomien $a_1(x), a_2(x), \ldots, a_n(x) \in F[x]$ *suurin yhteinen tekijä* on suuriasteisin pääpolynomi $c(x) \in F[x]$, jolle pätee $c(x) \mid a_i(x)$ kaikilla $i \in \{1, 2, \ldots, n\}$.

Huomautus. Matriisin A invarianteilla tekijöillä viitataan usein itse asiassa matriisin $xI - A$ invariantteihin tekijöihin.

Esimerkki 6.2. Vrt. [9, s. 680–681]. Tarkastelun kohteena on matriisi

$$A = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 0 & 0 & -4 \end{pmatrix}.$$

Ratkaistaan matriisin $xI - A$ invariantit tekijät kunnan $\mathbb{Q}$ suhteen. Rotman käyttää ratkaisussaan sekä alkeisoperaatioita että lauseen 6.4 tulosta. Tässä ratkaisussa hyödynnetään ainoastaan jälkimmäistä keinoa. Ensinnäkin

$$xI - A = \begin{pmatrix} x-2 & -3 & -1 \\ -1 & x-2 & -1 \\ 0 & 0 & x-(-4) \end{pmatrix} = \begin{pmatrix} x-2 & -3 & -1 \\ -1 & x-2 & -1 \\ 0 & 0 & x+4 \end{pmatrix}.$$

Määritelmän mukaan $d_0(xI - A) = 1$. Sen jälkeen on määritettävä $d_1(xI - A)$. Tämä saadaan selville tutkimalla 1×1-alimatriisien eli matriisin $xI - A$ alkioiden suurinta yhteistä tekijää. Koska alkioina esiintyvät esimerkiksi -3 ja -1, on selvää, että $d_1(xI - A) = 1$. Seuraavaksi on tarkasteltava matriisin $xI - A$ 2×2-kokoisia alimatriiseja. Yhteensä niitä on $3^2 = 9$ kappaletta. Huomataan muun muassa, että

$$\det \begin{pmatrix} x-2 & -1 \\ -1 & -1 \end{pmatrix} = -(x-2) - 1 = -x + 1$$

ja

$$\det \begin{pmatrix} -3 & -1 \\ x-2 & -1 \end{pmatrix} = 3 + (x-2) = x + 1.$$

Saadut determinantit ovat erisuuria jaottomia polynomeja, joten täytyy myös olla, että $d_2(xI - A) = 1$. Lopulta $d_3(xI - A)$ saadaan selville laskemalla normaalisti koko matriisin $xI - A$ determinantti:

$$\begin{aligned} \det(xI - A) &= (x+4)\big((x-2)^2 - 3\big) \\ &= (x+4)(x^2 - 4x + 4 - 3) \\ &= (x+4)(x^2 - 4x + 1) \\ &= x^3 - 4x^2 + x + 4x^2 - 16x + 4 \\ &= x^3 - 15x + 4. \end{aligned}$$

Polynomin $x^3-15x+4$ suurin yhteinen tekijä on se itse. Siis $d_3(xI-A) = x^3-15x+4$. Determinanttisten jakajien avulla on yksinkertaista selvittää invariantit tekijät. Ne saadaan aiemmin esitettyjä osamääriä käyttämällä:

$$\sigma_1 = \frac{d_1(xI-A)}{d_0(xI-A)} = \frac{1}{1} = 1, \qquad \sigma_2 = \frac{d_2(xI-A)}{d_1(xI-A)} = \frac{1}{1} = 1 \quad \text{ja}$$

$$\sigma_3 = \frac{d_3(xI-A)}{d_2(xI-A)} = \frac{x^3-15x+4}{1} = x^3-15x+4.$$

Huomaa, että yksiköillä kertominen tuottaa vaihtoehtoisia invariantteja tekijöitä.

Lause 6.6. *Olkoon F kunta, ja olkoot $A, B \in M_n(F)$. Tällöin kaksi samankokoista matriisia $\Gamma = xI - A, \Gamma' = xI - B \in M_n(F[x])$ on $F[x]$-ekvivalentit, jos ja vain jos niiden invariantit tekijät ovat samat. Oletetaan, että invariantit tekijät on esitetty pääpolynomeina.*

Todistus. Vrt. [3, s. 655]. Oletetaan aluksi, että Γ ja Γ' ovat $F[x]$-ekvivalentit. Määritelmän mukaan on olemassa kääntyvät matriisit $P, Q \in M_n(F[x])$, jotka toteuttavat yhtälön $\Gamma = Q\Gamma' P^{-1}$. Olkoon D matriisin Γ' Smithin normaalimuoto. Toisin sanoen

$$\Gamma' = RDS,$$

missä R ja S koostuvat alkeismatriisien tulosta. Havaitaan, että D on myös matriisin Γ Smithin normaalimuoto:

$$\Gamma = QRDSP^{-1}.$$

Tässä $P^{-1}, Q \in M_n(F[x])$, missä $F[x]$ on euklidinen alue, joten apulauseen 5.3 perusteella ne voidaan esittää alkeismatriisien tuloina. Koska oletetaan, että kaikki D:ssä esiintyvät invariantit tekijät ovat pääpolynomeja, Smithin normaalimuodon yksikäsitteisyyden nojalla matriisien Γ ja Γ' invariantit tekijät ovat samat.

Oletetaan sitten, että matriisien Γ ja Γ' invariantit tekijät ovat samat. Tällöin niillä on siis sama Smithin normaalimuoto D. Kirjoitetaan

$$\Gamma = E_1 D F_1 \quad \text{ja} \quad \Gamma' = E_2 D F_2,$$

missä E_1, E_2, F_1 ja F_2 ovat alkeismatriisien tuloina kääntyviä. Ratkaistaan jälkimmäisestä yhtälöstä D:

$$D = E_2^{-1}\Gamma' F_2^{-1}.$$

Nyt sijoittamalla saadaan

$$\Gamma = E_1 E_2^{-1}\Gamma' F_2^{-1} F_1.$$

Tässä matriisit $E_1E_2^{-1}, F_2^{-1}F_1 \in M_n(F[x])$ ovat kääntyvien matriisien tuloina kääntyviä, joten Γ ja Γ' ovat $F[x]$-ekvivalentit. □

Seuraus 6.7. Olkoon F kunta. Neliömatriisit $A, B \in M_n(F)$ ovat similaariset, jos ja vain jos matriiseilla $xI - A, xI - B \in M_n(F[x])$ on samat invariantit tekijät eli sama Smithin normaalimuoto, joka koostuu pääpolynomeista.

Todistus. Ks. lauseet 4.6 ja 6.6. □

Tarkastellaan kuntaa F ja joukkoa S, missä S on usein kunta F tai polynomirengas $F[x]$. Tällöin kuvausta $f : M_n(F) \to S$ kutsutaan $n \times n$-matriisien *similaarisuusinvariantiksi*, mikäli $f(A) = f(B)$ aina, kun A ja B ovat similaariset. Baker ja Porteous käsittelevät teoksessaan toistuvasti erilaisia similaarisuusinvariantteja (ks. etenkin [1, s. 217–225]). Yllä olevan seurauslauseen perusteella invariantit tekijät ovat $n \times n$-matriisien similaarisuusinvariantteja.

6.2 Alkeisjakajat

Tämä alaluku käsittelee lyhyesti alkeisjakajia, jotka voidaan invarianttien tekijöiden tavoin löytää saattamalla matriisin ensin Smithin normaalimuotoon. Toisaalta jos matriisin alkeisjakajat sekä aste ovat tiedossa, invariantit tekijät voidaan määrittää suhteellisen helposti. Matriisin aste kertoo nimittäin invarianttien tekijöiden lukumäärän.

Määritelmä 6.8. Vrt. [2, s. 330]. Olkoon $A \in M_{mn}(F[x])$, missä F on algebrallisesti suljettu kunta. Tällöin A:n jokainen invariantti tekijä σ_i voidaan kirjoittaa muodossa

$$\sigma_i = (x - \alpha_1)^{t_1}(x - \alpha_2)^{t_2} \cdots (x - \alpha_s)^{t_s}.$$

Tässä $(x - \alpha_1), (x - \alpha_2), \ldots, (x - \alpha_s)$ ovat invariantin tekijän erillisiä lineaarisia tekijöitä, ja t_j:t ovat ei-negatiivisia kokonaislukuja. Kaikkien matriisin A invarianttien tekijöiden epätriviaalien tekijöiden $(x - \alpha_j)^{t_j}, t_j \neq 0$, joukkoa kutsutaan *alkeisjakajien* joukoksi. Tässä joukossa voi esiintyä toistoja.

Esimerkki 6.3. Tiedetään, että matriisin $xI - A$ invariantit tekijät ovat

$$1, 1, 1, 1, 1, 1, x + 2, x^2 - 2x - 8, x^3 - 6x^2 + 32 \text{ ja } x^4 - 6x^3 + 32x.$$

Näistä epätriviaalit voidaan esittää myös muodossa

$$x + 2, \quad (x + 2)(x - 4), \quad (x + 2)(x - 4)^2 \quad \text{ja} \quad x(x + 2)(x - 4)^2.$$

Jälkimmäisestä esitystavasta on helppo muodostaa alkeisjakajien joukko. Luku 1 ei kuitenkaan kelpaa alkeisjakajaksi. Tässä esimerkissä alkeisjakajien joukossa esiintyy toistoja:

$$x + 2, \quad x + 2, \quad x - 4, \quad x + 2, \quad (x - 4)^2, \quad x, \quad x + 2, \quad (x - 4)^2.$$

Esimerkki 6.4. Tässä esimerkissä tarkastelut etenevät päinvastaiseen suuntaan kuin esimerkissä 6.3. Matriisin asteen tiedetään olevan kuusi. Päätellään seuraavaksi annettavien alkeisjakajien avulla matriisin kuusi invarianttia tekijää, joiden perusteella matriisi voidaan laittaa Smithin normaalimuotoon.

a) Alkeisjakajia ovat

$$x, \quad x^2, \quad x^2, \quad x-1, \quad x+3, \quad x-2.$$

Tehtävän voi ratkaista esimerkiksi käyttämällä apuna *pienimmän yhteisen jaettavan* käsitettä. Etsitään alkeisjakajien joukolle pienin yhteinen jaettava, jolloin saadaan määritettyä σ_6:

$$\sigma_6 = x^2(x-1)(x+3)(x-2).$$

Tämä todellakin on alkeisjakajien joukon pienin yhteinen jaettava, sillä σ_6 on pieniasteisin pääpolynomi, jonka jokainen alkeisjakaja jakaa. Huomaa, että tämä polynomien pienin yhteinen jaettava määritellään samaan tapaan kuin polynomien suurin yhteinen tekijä. Nyt alkeisjakajista neljä viimeistä on käytetty. Viidennen invariantin tekijän määrittämiseksi tarkastellaan jäljelle jääneiden alkeisjakajien pienintä yhteistä jaettavaa. Täten $\sigma_5 = x^2$. Vastaavasti päätellään, että $\sigma_4 = x$. Alkeisjakajien joukko on nyt käyty läpi, joten loppujen invarianttien tekijöiden on oltava ykkösiä:

$$\sigma_3 = \sigma_2 = \sigma_1 = 1.$$

b) Alkeisjakajien joukkoon kuuluvat

$$x-1, \quad (x-1)^2, \quad (x-1)^3, \quad (x-1)^4, \quad (x+1)^2.$$

Alkeisjakajia on viisi kappaletta, joten heti nähdään, että ainakin yhden invariantin tekijän on oltava 1. Samalla pienimmän yhteisen jaettavan tekniikalla kuin a)-kohdassa invarianteiksi tekijöiksi saadaan

$$\begin{aligned}
\sigma_1 &= 1 \\
\sigma_2 &= 1 \\
\sigma_3 &= x-1 \\
\sigma_4 &= (x-1)^2 \\
\sigma_5 &= (x-1)^3 \\
\sigma_6 &= (x-1)^4(x+1)^2.
\end{aligned}$$

Joseph J. Rotman tiivistää vielä algoritmimuodossa, miten alkeisjakajia voidaan määrittää (ks. [9, s. 680]). Olkoon $A \in M_n(F)$, missä F on jokin algebrallisesti suljettu kunta. Ensin etsitään matriisin $\Gamma = xI - A$ Smithin normaalimuoto. Tässä tutkielmassa on käsitelty kahta lähestymistapaa Smithin normaalimuotoon pääsemiseksi: Joko voi käyttää alkeisrivi- ja -sarakeoperaatioita matriisiin Γ, kuten lauseen 5.1 todistuksessa, tai lauseen 6.4 mukaista minoritekniikkaa. Ensimmäisessä menetelmässä suoritetaan alkeisoperaatioita, kunnes saavutetaan Smithin normaalimuoto ja algoritmi pysähtyy. Jälkimmäisessä on laskettava kaikki determinanttiset jakajat $d_i(\Gamma)$, $1 \leq i \leq n$, mikä osoittautuu varsin työlääksi suuria matriiseja käsiteltäessä.

Näin saadaan määritettyä ensin matriisin Γ invariantit tekijät. Nämä voidaan edelleen saattaa tekijöihinjakoalgoritmin avulla määritelmän 6.8 muotoon. Tässä vaiheessa ykkösen suuruiset invariantit tekijät voi unohtaa, sillä ne eivät tuota alkeisjakajia. Nyt invarianteissa tekijöissä esiintyvät muotoa $(x-\alpha)^t$ olevat tekijät muodostavat alkeisjakajien joukon, jossa saattaa esiintyä samoja alkioita useaan kertaan.

7 Smithin normaalimuodon käyttö

Tämän viimeisen luvun tavoitteena on antaa muutamia konkreettisia esimerkkejä Smithin normaalimuodon käytöstä. Ensin tarkastellaan, mitä seikkoja Smithin normaalimuodosta on mahdollista saada selville. Tämän jälkeen esitetään, kuinka lineaarisia yhtälöryhmiä pystytään tarvittaessa ratkaisemaan saattamalla vastaava matriisi ensin haluttuun muotoon. Viimeinen sovellus koskee matriisien permutaatioekvivalenttiuden selvittämistä.

Esitetään joitakin pieniä, mutta mielenkiintoisia yksityiskohtia faktoina ilman todistusta (ks. [1, s. 233–234]). Olkoon A $n \times n$-matriisi. Olkoot $\sigma_1, \sigma_2, \ldots, \sigma_n$ matriisin $xI - A$ pääpolynomeiksi valittuja invariantteja tekijöitä. Huomaa, että tässä tarkastelussa invariantteja tekijöitä on n kappaletta, koska $\det(xI - A) = \mathrm{ch}(A)$ ja karakteristinen polynomi ei voi olla nolla. Täten matriisin $xI - A$ Smithin normaalimuodossa ei voi esiintyä nollarivejä tai -sarakkeita. Nyt

a) Matriisin A karakteristinen polynomi on invarianttien tekijöiden tulo

$$\mathrm{ch}(A) = \prod_{i=1}^{n} \sigma_i.$$

b) Matriisin A minimaalipolynomi on viimeinen invariantti tekijä $\min(A) = \sigma_n$.

c) Matriisin A determinantti $\det(A)$ on lauseke $(-1)^n \mathrm{ch}(A)$ arvolla $x = 0$ eli toisin sanoen $(-1)^n$ kertaa karakteristisen polynomin vakiotermi.

d) Matriisin A jälki $\mathrm{tr}(A)$ on karakteristisen polynomin $(n-1)$. asteen termin x^{n-1} kertoimen vastaluku.

e) Matriisin A aste $\mathrm{rank}(A)$ on sellaisten invarianttien tekijöiden σ_i lukumäärä, joiden vakiotermi ei ole nolla.

Esimerkki 7.1. Esimerkissä 6.2 tarkasteltiin matriisia

$$A = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 1 \\ 0 & 0 & -4 \end{pmatrix}$$

ja määritettiin matriisin $xI - A$ invariantit tekijät. Saatiin yhteensä kolme invarianttia tekijää: $\sigma_1 = \sigma_2 = 1$ ja $\sigma_3 = x^3 - 15x + 4$. Nämä ovat pääpolynomeja, kuten halutaan. Matriisin A karakteristinen polynomi on nyt

$$\mathrm{ch}(A) = 1 \cdot 1 \cdot (x^3 - 15x + 4) = x^3 - 15x + 4.$$

Kolmas ja viimeinen invariantti tekijä on $\sigma_3 = x^3 - 15x + 4$, joka on myös A:n minimaalipolynomi. Matriisin A determinantti on helppo selvittää ilman sen suurempia laskutoimituksia edellä todetun perusteella:

$$\det(A) = (-1)^3 \cdot (0^3 - 15 \cdot 0 + 4) = -1 \cdot 4 = -4.$$

Samaan päädytään, jos lasketaan determinantti normaaliin tapaan 3×3-matriisista.

Tässä tapauksessa A:n jälki olisi muutenkin hyvin helppo laskea, mutta lisäksi d)-kohdan perusteella voidaan tutkia karakteristisen polynomin toisen asteen termin kerrointa. Koska se on nolla, ja nollan vastaluku on myös nolla, matriisin A jälki on $\operatorname{tr}(A) = 0$. Kaikkien kolmen invariantin tekijän vakiotermi on nollasta poikkeava, joten matriisin A asteeksi saadaan $\operatorname{rank}(A) = 3$.

Smith keksi normaalimuotonsa alun perin ratkaistakseen lineaarisia yhtälöryhmiä. Hän tarkasteli *lineaarisia Diofantoksen yhtälöitä*, jotka ovat kokonaislukukertoimisia vähintään kahden muuttujan ensimmäisen asteen yhtälöitä. Seuraavaksi esitetäänkin tekniikka, jolla Smithin normaalimuodon avulla voidaan ratkaista tällaisista yhtälöistä koostuva yhtälöryhmä (vrt. [7, s. 372]).

Tutkitaan matriisia $A \in M_{mn}(\mathbb{Z})$ ja vektoria $b \in M_{m1}(\mathbb{Z})$. Tavoitteena on löytää kaikki kokonaislukuratkaisut Diofantoksen yhtälöryhmälle $Ax = b$. Ensin etsitään matriisille A Smithin normaalimuoto $S = UAV$, missä U ja V ovat alkeismatriisien tuloja. U edustaa matriisille suoritettavia alkeisrivioperaatioita ja V puolestaan alkeissarakeoperaatioita.

Korvataan sitten $Ax = b$ ekvivalentilla yhtälöryhmällä $Sy = c$, missä $x = Vy$ ja $c = Ub$. Kyseessä todellakin ovat ekvivalentit yhtälöryhmät, sillä U ja V ovat alkeismatriisien tuloina kääntyviä, yhtälö $y = V^{-1}x$ pätee ja

$$\begin{aligned} Sy = c \quad &\Leftrightarrow \\ SV^{-1}x = c \quad &\Leftrightarrow \\ SV^{-1}x = Ub \quad &\Leftrightarrow \\ U^{-1}SV^{-1}x = b \quad &\Leftrightarrow \\ Ax = b. \quad & \end{aligned}$$

Merkitään $r = \operatorname{rank}(A)$. Tällöin

$$S = \begin{pmatrix} D & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix},$$

missä D on Smithin normaalimuodon $r \times r$-lävistäjäosa. Merkitään seuraavaksi vektoreita $c = (c', c'')^\top$ ja $y = (y', y'')^\top$, missä $\top$ tarkoittaa transpoosia. Tässä c' ja y' ovat $r \times 1$-vektoreita. Sen sijaan c'' on $(m - r) \times 1$-vektori, ja y'' on $(n - r) \times 1$-vektori. Mikäli $r = m$, vektorissa c ei esiinny lainkaan c'':a. Vastaavasti, jos $r = n$, vektorissa y ei ole y'':a. Sekä c'' että y'' puuttuvat, jos $r = m = n$ eli A on niin sanottu *täysiasteinen* neliömatriisi. Nyt

$$Sy = \begin{pmatrix} D & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} y' \\ y'' \end{pmatrix} = \begin{pmatrix} Dy' \\ \mathbf{0} \end{pmatrix},$$

joten $Sy = c$, jos ja vain jos $c' = Dy'$ ja $c'' = \mathbf{0}$. Täten yhtälöryhmällä on kokonaislukuratkaisuja, jos ja vain jos $c'' = \mathbf{0}$ ja $y' = D^{-1}c'$ on rationaaliluvuista koostuva vektori. Merkitään $y = (y_1, y_2, \ldots, y_r, y_{r+1}, \ldots, y_n)^\top$. Kaikkien ratkaisujen selvittämiseksi olkoot alkiot $y_{r+1}, \ldots, y_n$ mielivaltaisia kokonaislukuja, jotka muodostavat

y'':n. Jos näitä alkioita ylipäätään on, ne esiintyvät yhtälöryhmän yleisessä ratkaisussa, joka käsittää kaikki Diofantoksen yhtälöryhmän $Ax = b$ toteuttavat vektorit x. Sijoittamalla eri kokonaislukuja mielivaltaisten alkioiden paikalle saadaan yhtälöryhmälle useita eri ratkaisuja. Yksi lineaarisen Diofantoksen yhtälöryhmän ratkaisu on muotoa

$$x = Vy = V(y', y'')^\top = V(D^{-1}c', \mathbf{0})^\top,$$

mihin on sijoitettu $n - r$ nollaa vektorin y osaan y''. Nollat voisi kuitenkin korvata millä tahansa kokonaisluvuilla, ja edelleen saataisiin jokin toinen yhtälöryhmän ratkaisu.

Esimerkki 7.2. Olkoon

$$A = \begin{pmatrix} 2 & 1 & 0 & 7 \\ -3 & 4 & 0 & 6 \\ 2 & -1 & 0 & 1 \end{pmatrix} \quad \text{ja} \quad b = \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix}.$$

Tavoitteena on etsiä kaikki kokonaislukuratkaisut yhtälöryhmälle $Ax = b$, joka voidaan myös esittää muodossa

$$\begin{cases} 2x_1 + x_2 + 7x_4 &= 3 \\ -3x_1 + 4x_2 + 6x_4 &= 1 \\ 2x_1 - x_2 + x_4 &= 1 \end{cases},$$

kun merkitään, että $x = (x_1, x_2, x_3, x_4)^\top$. Selvitetään ensin, mikä on matriisin A aste. Suurin vaihtoehto on, että se on kolme. Havaitaan kuitenkin, että aina, kun A:n kolmas sarake otetaan mukaan 3×3-alimatriisiin, determinantiksi tulee nolla. Tarkastetaan erikseen nollattoman 3×3-alimatriisin determinantti:

$$\begin{aligned} \det \begin{pmatrix} 2 & 1 & 7 \\ -3 & 4 & 6 \\ 2 & -1 & 1 \end{pmatrix} &= 2 \cdot \det \begin{pmatrix} 4 & 6 \\ -1 & 1 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} -3 & 6 \\ 2 & 1 \end{pmatrix} + 7 \cdot \det \begin{pmatrix} -3 & 4 \\ 2 & -1 \end{pmatrix} \\ &= 2 \cdot 10 - 1 \cdot (-15) + 7 \cdot (-5) \\ &= 20 + 15 - 35 \\ &= 0. \end{aligned}$$

Kaikkien 3×3-alimatriisien determinantti on siis nolla, joten matriisin A aste ei voi olla kolme. Sen sijaan esimerkiksi

$$\det \begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} = 8 + 3 = 11 \neq 0,$$

joten $\operatorname{rank}(A) = 2$.

Suorittamalla esimerkiksi seuraavat yhdeksän operaatiota matriisille A se saadaan Smithin normaalimuotoon:

1) Vaihdetaan SARAKE(1) ja SARAKE(2) keskenään.
2) Vaihdetaan SARAKE(3) ja SARAKE(4) keskenään.
3) Korvataan RIVI(2) summalla RIVI(2)+(-4)RIVI(1).
4) Korvataan RIVI(3) summalla RIVI(3)+RIVI(1).
5) Korvataan SARAKE(2) summalla SARAKE(2)+(-2)SARAKE(1).

6) Korvataan SARAKE(3) summalla SARAKE(3)+(-7)SARAKE(1).
7) Korvataan RIVI(2) summalla RIVI(2)+3·RIVI(3).
8) Korvataan RIVI(3) summalla RIVI(3)+(-4)RIVI(2).
9) Korvataan SARAKE(3) summalla SARAKE(3)+(-2)SARAKE(2).

Esitetään vielä matriiseina, miten Smithin normaalimuotoon päädytään:

$$\begin{pmatrix} 2 & 1 & 0 & 7 \\ -3 & 4 & 0 & 6 \\ 2 & -1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 0 & 7 \\ 4 & -3 & 0 & 6 \\ -1 & 2 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 7 & 0 \\ 4 & -3 & 6 & 0 \\ -1 & 2 & 1 & 0 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 2 & 7 & 0 \\ 0 & -11 & -22 & 0 \\ -1 & 2 & 1 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 7 & 0 \\ 0 & -11 & -22 & 0 \\ 0 & 4 & 8 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 7 & 0 \\ 0 & -11 & -22 & 0 \\ 0 & 4 & 8 & 0 \end{pmatrix} \to$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -11 & -22 & 0 \\ 0 & 4 & 8 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 4 & 8 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Jos merkitään Smithin normaalimuotoa kirjaimella S, saadaan yhtälö $S = UAV$, missä U ja V ovat alkeismatriisien tuloja. Merkitään lisäksi, että

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

on Smithin normaalimuodon lävistäjäosa.

Määritetään seuraavaksi matriisit U ja V. Ensin on muodostettava kutakin alkeisoperaatiota vastaavat matriisit. U edustaa alkeisrivioperaatiomatriisien tuloa ja V puolestaan alkeissarakeoperaatiomatriisien tuloa. U:n määrityksessä on keskeistä huomata, että alkeisrivioperaatioita suoritettaessa käsiteltävä matriisi kerrotaan aina vasemmalta. Koska matriisikertolasku ei yleensä ole vaihdannainen, alkeisrivioperaatioita vastaavat matriisit on asetettava "käänteiseen" järjestykseen:

$$U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 3 \\ 5 & -4 & -11 \end{pmatrix}.$$

Neljästä kerrottavasta matriisista ensimmäistä vastaava alkeisrivioperaatio siis suoritetaan viimeisenä ja niin edelleen. Matriisikertolasku on sen sijaan liitännäinen, joten neljää matriisia kerrottaessa sulutuksen voi päättää itse. Matriisin V tapauksessa kertolaskujärjestys on luonnollinen, sillä alkeissarakeoperaatioiden yhteydessä kertolasku tapahtuu oikealta. Matriisi V saadaan seuraavan matriisikertolaskun tuloksena:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -7 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Näin ollen

$$V = \begin{pmatrix} 0 & 1 & -2 & 0 \\ 1 & -2 & -3 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Seuraavaksi ratkaistaan vektori c. Koska c on määritelty tunnettujen elementtien U ja b avulla, saadaan

$$c = Ub = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 3 \\ 5 & -4 & -11 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix},$$

missä $c' = (3, 1)^\top$. Nyt

$$D^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

joten

$$y' = D^{-1}c' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

ja $y = (3, 1, s, t)^\top$, missä $s, t \in \mathbb{Z}$. Tällöin kaikki yhtälöryhmän $Ax = b$ ratkaisut ovat

$$x = Vy = \begin{pmatrix} 0 & 1 & -2 & 0 \\ 1 & -2 & -3 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ s \\ t \end{pmatrix} = \begin{pmatrix} 1 - 2s \\ 1 - 3s \\ t \\ s \end{pmatrix}.$$

Yksi ratkaisu saadaan, kun sijoitetaan, että $s = t = 0$, jolloin

$$x = \begin{pmatrix} 1 - 2 \cdot 0 \\ 1 - 3 \cdot 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Lopuksi käsitellään vielä sovellusta permutaatioekvivalenttiudesta. Oletetaan, että tehtävänä on selvittää, onko kaksi matriisia permutaatioekvivalentit eli voidaanko ensimmäisestä saada toinen vaihtamalla rivejä tai sarakkeita sopivasti keskenään. Permutaatioekvivalenttiutta voi toki lähteä tarkistamaan systemaattisesti, mutta suurten matriisien kohdalla tämä ei kuitenkaan käytännössä ole mahdollista.

Tarkastellaan tilannetta, jossa F on kunta ja $A, B \in M_n(F)$. Halutaan selvittää, ovatko matriisit $\Gamma = xI - A, \Gamma' = xI - B \in M_n(F[x])$ permutaatioekvivalentit. Helppo keino todeta, että ne eivät ole permutaatioekvivalentteja, on tarkastella matriisien Γ ja Γ' Smithin normaalimuotoja – tarkemmin sanottuna niiden invariantteja tekijöitä. Lauseen 6.6 perusteella tiedetään nimittäin, että mikäli invariantit tekijät eivät ole samat, Γ ja Γ' eivät ole $F[x]$-ekvivalentteja keskenään. Lisäksi permutaatioekvivalentit matriisit ovat aina myös ekvivalentteja (tässä $F[x]$-ekvivalentteja).

Kun käytetään jälkimmäisen kontrapositiota, invarianttien tekijöiden erisuuruudesta voi päätellä, että matriisit Γ ja Γ' eivät ole permutaatioekvivalentteja keskenään (vrt. [7, s. 373–375]). Esitetään tästä vielä konkreettinen esimerkki.

Esimerkki 7.3. Olkoot

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 3 & 2 & 1 \\ 2 & 3 & 3 \end{pmatrix} \quad \text{ja} \quad B = \begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}, \quad \text{missä alkiot ovat reaalilukuja.}$$

Tällöin

$$\Gamma = xI - A = \begin{pmatrix} x-1 & -2 & -1 \\ -3 & x-2 & -1 \\ -2 & -3 & x-3 \end{pmatrix} \text{ ja } \Gamma' = xI - B = \begin{pmatrix} x-2 & -3 & -1 \\ -3 & x-1 & -2 \\ -1 & -2 & x-3 \end{pmatrix}.$$

Tehtävänä on selvittää, ovatko Γ ja Γ' permutaatioekvivalentit. Etsitään ensin kummankin matriisin invariantit tekijät, sillä mikäli ne osoittautuvat erisuuriksi, voimme heti päätellä, että matriisit Γ ja Γ' eivät ole permutaatioekvivalentteja edellä esitetyn nojalla. Käytetään apuna lauseen 6.4 tulosta.

Aloitetaan matriisin Γ invarianteista tekijöistä. On ensinnäkin määritelty, että $d_0(\Gamma) = 1$. Myös $d_1(\Gamma) = 1$, koska tarkasteltavana on Γ:n kaikkien yhdeksän alkion suurin yhteinen tekijä. Koska esimerkiksi -1 ja -2 ovat matriisin alkioita, suurin yhteinen tekijä on tietenkin 1. Tutkitaan sitten 2×2-alimatriisien determinantteja. Esimerkiksi

$$\det \begin{pmatrix} x-1 & -2 \\ -3 & x-2 \end{pmatrix} = (x-1)(x-2) - 6 = x^2 - 3x - 4 = (x+1)(x-4) \quad \text{ja}$$

$$\det \begin{pmatrix} x-1 & -1 \\ -3 & -1 \end{pmatrix} = -(x-1) - 3 = -x - 2 = -(x+2).$$

Jo näiden minorien perusteella voidaan sanoa, että suurin yhteinen tekijä on yksi eli $d_2(\Gamma) = 1$. Lasketaan lopuksi vielä koko matriisin Γ determinantti $\det(\Gamma)$:

$$(x-1) \cdot \det \begin{pmatrix} x-2 & -1 \\ -3 & x-3 \end{pmatrix} + 2 \cdot \det \begin{pmatrix} -3 & -1 \\ -2 & x-3 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} -3 & x-2 \\ -2 & -3 \end{pmatrix}$$

$$\begin{aligned} &= (x-1)\big((x-2)(x-3) - 3\big) + 2\big(-3(x-3) - 2\big) - \big(9 + 2(x-2)\big) \\ &= (x-1)(x^2 - 5x + 3) + 2(-3x + 7) - (2x + 5) \\ &= x^3 - 5x^2 + 3x - x^2 + 5x - 3 - 6x + 14 - 2x - 5 \\ &= x^3 - 6x^2 + 6 = d_3(\Gamma). \end{aligned}$$

Siis matriisin Γ invariantit tekijät ovat

$$\sigma_1 = \frac{1}{1} = 1, \quad \sigma_2 = \frac{1}{1} = 1 \quad \text{ja} \quad \sigma_3 = \frac{x^3 - 6x^2 + 6}{1} = x^3 - 6x^2 + 6.$$

Määritetään sitten matriisin Γ' invariantit tekijät samaan tapaan. Myös tässä tapauksessa tiedetään, että $d_0(\Gamma') = d_1(\Gamma') = 1$. Koska esimerkiksi

$$\det \begin{pmatrix} -3 & x-1 \\ -1 & -2 \end{pmatrix} = 6 + (x-1) = x + 5 \quad \text{ja}$$

$$\det \begin{pmatrix} -3 & -1 \\ -2 & x-3 \end{pmatrix} = -3(x-3) - 2 = -3x + 7,$$

2×2-minorien suurin yhteinen tekijä on yksi, ja näin ollen $d_2(\Gamma') = 1$. Lopuksi määritetään $\det(\Gamma')$, joka on sama kuin $d_3(\Gamma')$:

$$(x-2) \cdot \det \begin{pmatrix} x-1 & -2 \\ -2 & x-3 \end{pmatrix} + 3 \cdot \det \begin{pmatrix} -3 & -2 \\ -1 & x-3 \end{pmatrix} - 1 \cdot \det \begin{pmatrix} -3 & x-1 \\ -1 & -2 \end{pmatrix}$$

$$\begin{aligned}
&= (x-2)\big((x-1)(x-3) - 4\big) + 3\big(-3(x-3) - 2\big) - \big(6 + (x-1)\big) \\
&= (x-2)(x^2 - 4x - 1) + 3(-3x + 7) - x - 5 \\
&= x^3 - 4x^2 - x - 2x^2 + 8x + 2 - 9x + 21 - x - 5 \\
&= x^3 - 6x^2 - 3x + 18.
\end{aligned}$$

Matriisin Γ' invarianteiksi tekijöiksi saadaan

$$\sigma'_1 = \frac{1}{1} = 1, \quad \sigma'_2 = \frac{1}{1} = 1 \quad \text{ja} \quad \sigma'_3 = \frac{x^3 - 6x^2 - 3x + 18}{1} = x^3 - 6x^2 - 3x + 18.$$

Nyt sekä matriisin Γ että Γ' invariantit tekijät on valittu pääpolynomeiksi, joten ne ovat yksikäsitteisiä. Koska $x^3 - 6x^2 + 6 \neq x^3 - 6x^2 - 3x + 18$, niin Γ:n ja Γ':n invariantit tekijät eivät ole samat. Siksi matriisit Γ ja Γ' eivät ole $\mathbb{R}[x]$-ekvivalentteja, eivätkä täten permutaatioekvivalentteja.

Edellä esitettyjen sovellusten lisäksi Smithin normaalimuotoa voi hyödyntää esimerkiksi kongruenssiyhtälön $Ax \equiv b \mod l$ ratkaisemisessa. Tässä l on mikä tahansa positiivinen kokonaisluku. Tällainen kongruenssiyhtälö voidaan ratkaista samaan tapaan kuin lineaarinen yhtälöryhmä. Smithin normaalimuotoa käytetään myös ryhmäteoriassa. (Ks. [4, s. 558] ja [7, s. 376–378]).

Lähteet

[1] Baker, A. C. ja Porteous, H. L. *Linear Algebra and Differential Equations*. Ellis Horwood Limited, 1990.

[2] Barnett, S. *Matrices: Methods and Applications*. Oxford University Press, 1990.

[3] Gohberg, I., Lancaster, P. ja Rodman, L. *Invariant Subspaces of Matrices with Applications*. The Society for Industrial and Applied Mathematics, 2006.

[4] Ilmonen, P. ja Haukkanen, P. *Smith meets Smith: Smith normal form of Smith matrix*. Linear and Multilinear Algebra 59 (2011) 557–564.

[5] Lang, S. *Linear Algebra*. 2. painos. Addison-Wesley Publishing Company, 1967.

[6] Malik, D. S., Mordeson, J. N. ja Sen, M. K. *Fundamentals of Abstract Algebra*. McGraw-Hill, 1997.

[7] Newman, M. *The Smith Normal Form*. Linear Algebra Appl. 254 (1997) 367–381.

[8] Roman, S. *Advanced Linear Algebra*. Springer-Verlag, 1992.

[9] Rotman, J. J. *Advanced Modern Algebra*. 2. painos. American Mathematical Society, 2010.

[10] Wyels, C. J. *Permutation Equivalence and the Hermite Invariant*. Linear Algebra Appl. 256 (1997) 125–140.

[11] Zhan, X. *Matrix Theory*. American Mathematical Society, 2013.